625-CD-004-002

EOSDIS Core System Project

ECS Project Training Material
Volume 4: System Administration

March 1999

Raytheon Systems Company
Upper Marlboro, Maryland

ECS Project Training Material
Volume 4: System Administration

March 1999

Prepared Under Contract NAS5-60000
CDRL Item 129

RESPONSIBLE ENGINEER

Michael J. Blumenthal /s/ 3/22/99

Michael J. Blumenthal Date
EOSDIS Core System Project

SUBMITTED BY

Thomas J. Hickey /s/ 3/23/99

Tom Hickey, M&O Manager Date
EOSDIS Core System Project

Raytheon Systems Company
Upper Marlboro, Maryland

625-CD-004-002

This page intentionally left blank.

Preface

This document is a contract deliverable with an approval code of 3. As such, it does not require formal Government approval. This document is delivered for information only, but is subject to approval as meeting contractual requirements.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Raytheon Systems Company
1616 McCormick Dr.
Upper Marlboro, MD 20774-5301

This page intentionally left blank.

Abstract

This is Volume 4 of a series of lessons containing the training material for Release 4 of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). This lesson provides a detailed description of the process required for submitting and updating trouble tickets as well as investigating problems and identifying and implementing solutions.

***Keywords**:* training, instructional design, course objective, problem management, trouble ticket, trouble ticket review board, failure review board, Remedy.

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Revised
iii through xiv	Revised
1 through 126	Revised
Slide Presentation 1 through 90	Revised

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
625-CD-004-001	Original	December 1997	
625-CD-004-002	Revised	March 1999	

This page intentionally left blank.

Contents

System Startup and Shutdown

The ECS Assistant

HP OpenView - Network Node Manager

Secure Shell (ssh)

Tape Operations

System Backups and Restores

System Log Maintenance

User Administration

New Workstation Installation

Contractor Off-the-Shelf (COTS) Administration

Distributed Computing Environment (DCE)

Security

Practical Exercises

Slide Presentation

This page intentionally left blank.

Introduction

Identification

Training Material Volume 4 is part of Contract Data Requirements List (CDRL) Item 129, whose requirements are specified in Data Item Description (DID) 625/OP3 and is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract (NAS5-6000).

Scope

Training Material Volume 4: System Administration defines the steps required to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

Purpose

The purpose of this Student Guide is to provide a detailed course of instruction that forms the basis for understanding Network Administration. Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

Status and Schedule

This lesson module provides detailed information about training for Release 4. Subsequent revisions will be submitted as needed.

Organization

This document is organized as follows:

Introduction:	The Introduction presents the document identification, scope, purpose, and organization.
Related Documentation:	Related Documentation identifies parent, applicable and information documents associated with this document.
Student Guide:	The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics are included.
Slide Presentation:	Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson.

This page intentionally left blank.

Related Documentation

Parent Document

The parent document is the document from which this ECS Training Material's scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work

Applicable Documents

The following documents are referenced within this ECS Training Material, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this document:

423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)
420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)

Information Documents

Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

609-CD-003	Operations Tools Manual for the ECS Project
611-CD-004	Mission Operation Procedures for the ECS Project
535-TIP-CPT-001	Goddard Space Flight Center, Mission Operations and Data Systems Directorate (MO&DSD) Technical Information Program Networks Technical Training Facility, Contractor-Provided Training Specification

Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

220-TP-001	Operations Scenarios - ECS Release B.0 Impacts, Technical Paper for the ECS Project
305-CD-020	Release B SDPS/CSMS System Design Specification Overview for the ECS Project
305-CD-021	Release B SDPS Client Subsystem Design Specification for the ECS Project
305-CD-022	Release B SDPS Interoperability Subsystem Design Specification for the ECS Project
305-CD-023	Release B SDPS Data Management Subsystem Design Specification for the ECS Project
305-CD-024	Release B SDPS Data Server Subsystem Design Specification for the ECS Project
305-CD-025	Release B SDPS Ingest Subsystem Design Specification [for the ECS Project
305-CD-026	Release B SDPS Planning Subsystem Design Specification for the ECS Project
305-CD-027	Release B SDPS Data Processing Subsystem Design Specification for the ECS Project
305-CD-028	Release B CSMS Communications Subsystem Design Specification for the ECS Project
305-CD-029	Release B CSMS System Management Subsystem Design Specification for the ECS Project
305-CD-030	Release B GSFC DAAC Design Specification for the ECS Project
305-CD-031	Release B Langley DAAC Design Specification for the ECS Project
305-CD-033	Release B EDC DAAC Design Specification for the ECS Project
305-CD-034	Release B ASF DAAC Design Specification for the ECS Project
305-CD-035	Release B NSIDC DAAC Design Specification for the ECS Project
305-CD-036	Release B JPL PO.DAAC Design Specification for the ECS Project
305-CD-037	Release B ORNL DAAC Design Specification for the ECS Project
305-CD-038	Release B System Monitoring and Coordination Center Design Specification for the ECS Project

305-CD-039	Release B Data Dictionary Subsystem Design Specification for the ECS Project
601-CD-001	Maintenance and Operations Management Plan for the ECS Project
604-CD-001	Operations Concept for the ECS Project: Part 1-- ECS Overview
604-CD-002	Operations Concept for the ECS Project: Part 2B -- ECS Release B
605-CD-002	Release B SDPS/CSMS Operations Scenarios for the ECS Project
607-CD-001	ECS Maintenance and Operations Position Descriptions
500-1002	Goddard Space Flight Center, Network and Mission Operations Support (NMOS) Certification Program, 1/90

This page intentionally left blank.

System Administration

Lesson Overview

This lesson will provide you with the tools needed to perform the various tasks required to administer Implementation of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) during maintenance and operations.

Lesson Objectives

Overall Objective - The overall objective of his lesson is proficiency in the various tasks required to administer the ECS during maintenance and operations.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will use the Procedures Manual in accordance with prescribed methods and complete required procedures without error to accomplish all tasks required.

Specific Objective 1 - The student will startup and shutdown the ECS in its entirety.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to effect a complete startup and a complete and orderly shutdown of the ECS.

Specific Objective 2 - The student will manually shutdown and restart a single subsystem of the ECS without affecting other subsystems.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to effect an orderly shutdown and startup of one subsystem of the ECS without compromising or otherwise affecting the other component subsystems from the command line.

Specific Objective 3 - The student will shutdown and restart a single subsystem of the ECS using ECS Assistant without affecting other subsystems.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to effect an orderly shutdown and startup of one subsystem of the ECS without compromising or otherwise affecting the other component subsystems using the ECS Assistant.

Specific Objective 4 - The student will be able to label and index a tape cartridge.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to label a tape and index a tape cartridge.

Specific Objective 5 - The student will be able to create an incremental tape backup.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to create an incremental tape backup of system files created or modified within the past six days.

Specific Objective 6 - The student will be able to create a tape backup of the entire ECS system.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform a complete tape backup of the ECS.

Specific Objective 7 - The student will be able to restore individual files or entire volumes of backup tapes to the ECS system.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform individual or complete file restorations.

Specific Objective 8 - The student will be able to review and modify system logs.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to perform system log maintenance.

Specific Objective 9 - The student will create, modify, and delete user accounts on the ECS.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to add a new user account to the ECS, make modifications to a variety of account access parameters, and delete the account from the ECS.

Specific Objective 10 - The student will be able to check and modify access privileges on files and directories across the ECS.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to check file and directory access privileges and modify them to allow or deny access by various classes of users.

Specific Objective 11 - The student will be able to install, configure, and test a new workstation.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to install, configure, and test a new workstation including installing COTS, custom software, operating systems.

Specific Objective 12 - The student will be able to determine when security breaches occur and will be able to remedy such breaches.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to identify when security breaches occur and to remedy such breaches.

Specific Objective 13 - The student will be able to install, configure, and test DCE software.

Condition - The student will be given a copy of *625-CD-004-001 ECS Project Training Material Volume 4: System Administration* and a functioning system.

Standard - The student will perform without error the procedures required to install, configure, and test DCE software.

Importance

A System Administrator's goal is to keep the computer system usable by the users. A system running at peak efficiency does so because of the proper use of the tools provided for and used by the System Administrator. Intimate knowledge of how each tool works and which should be used in a particular situation is crucial to satisfying the ECS user community.

This page intentionally left blank.

System Startup and Shutdown

Overview

Starting or shutting down a computer system may involve nothing more than turning a power switch to the on or off position. However, the interdependency of the various servers may require the System Administrator to startup or shutdown the servers in a particular order. Depending on the situation, the entire computer system may be started or stopped (cold) or only selected servers may be started or stopped (warm). The next sections cover the procedures and details of cold and warm startups and shutdowns.

A complete system startup and shutdown should only need to occur approximately once in three or four months during the early stages of system implementation due to the inherent instability of new systems. After the system stabilizes, it is estimated that complete system startups and shutdowns will occur only about once a year. Partial shutdowns and restarts will be performed as needed due to maintenance concerns.

Cold Startup By Subsystem

A cold startup is indicated when there are no subsystems currently running, such as when the system is to be turned on for the first time, following a system maintenance operation that requires all power to be turned off, or following a power failure. In most situations a cold startup is also indicated by the power switch being in the OFF position.

The Cold System Startup is done in sequential order by subsystem. Figure 1 below shows the order at the DAAC in which each server is to be booted to achieve a fully functional system.

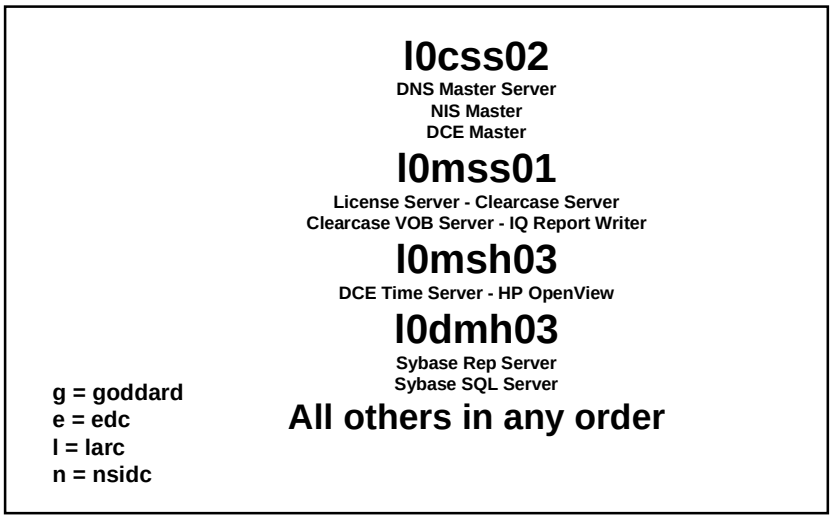

Figure 1. DAAC Server Startup Order

Cold Subsystem Startup Procedure

1	Determine which machines perform the following functions. Some may perform multiple functions: • Domain Name Server (DNS) Master • Name Information Server (NIS) Master • Mail Hub Server(s) • Automount Servers • Clearcase Server • Communication Subsystem (CSS) including Distributed Computing Environment (DCE) Server • DCE License Server for SUN • Other License Servers • System Management Subsystem • Sybase SQL Servers • Data Server Subsystem (DSS) • Planning & Data Processing System (PDPS) • Client, Interoperability and Data Management (CIDM) Subsystem
2	Startup the DNS Master. Once the system has booted without error, proceed to step 3.
3	Power on the NIS Master. Once the system has booted without error, proceed to step 4.
4	Power on the Mail Hub server(s). Once the system(s) have booted without error, proceed to step 5.
5	Power on the Automount/Mail HUB server(s). Once the system(s) have booted without error, proceed to step 6.
6	Power on the Clearcase server(s). Once the systems(s) have booted without error, proceed to step 7.
7	Power on the CSS server(s). Once the system(s) have booted without error, proceed to step 8.
8	Power on the DCE License server for SUN. Once the system has booted without error, proceed to step 9.
9	Power on the Other License server(s). Once the system(s) have booted without error, proceed to step 10.
10	Power on the MSS server(s). Once the system(s) have booted without error, proceed to step 11.
11	Power on the DSS server(s). Once the system(s) have booted without error, proceed to step 12.

12 Power on the PDPS server(s). Once the system(s) have booted without error, proceed to step 13.

13 Power on the CIDM server(s).

Warm Startup

A warm startup is indicated when there are some subsystems currently running while others have been shutdown either due to operator intervention or an external malfunction. The subsystems not actively running need to be started without interfering with the current active operations. In some instances, a warm startup may require some active subsystems to be shutdown and restarted so that their interaction and connectivity will be properly resumed.

Warm Subsystem Startup Procedure

1 Determine which machines perform the following functions:

- Domain Name Server (DNS) Master
- Name Information Server (NIS) Master
- Mail Hub Server(s)
- Automount Servers
- Clearcase Server
- Communication Subsystem (CSS) including Distributed Computing Environment (DCE) Server
- DCE License Server for SUN
- Other License Servers
- System Management Subsystem
- Sybase SQL Servers
- Data Server Subsystem (DSS)
- Planning & Data Processing System (PDPS)
- Client, Interoperability and Data Management (CIDM) Subsystem

2 Determine which machine is currently down.

3 Determine the interoperability dependencies among the machines.

4 Turn on machines in an order consistent with the dependencies.

Note - in addition to warm system startup/reboot sequences, ECS servers which use the Sybase SQL server may need to be bounced whenever the SQL server is bounced. At present, this is

certainly the case for all STMGT servers. That is, if the Sybase SQL server is stopped and restarted for any reason, all STMGT servers need to be stopped and restarted, once the Sybase SQL server has come back on-line.

Aditional tasking - Updating leapsec.dat and utcpole.dat files

In addition to starting system servers there are essential tasks that System Administrators must perform on a regular basis.

In order to ensure proper operation of Program Generated Executives (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are ${PGSHOME}/database/common/TD/leapsec.dat and ${PGSHOME}/database/common/CSC/utcpole.dat. The update of these files is accomplished by executing leapsec_update.sh and utcpole_update.sh in the /tools/admin/exec directory with root privileges. It has not been determined yet if these tasks will be accomplished manually or via cron job scripting .

Normal Shutdown

A normal shutdown occurs when the operator is required to turn off the power to the entire system or any of the component subsystems. Normal shutdowns are scheduled by the Resource Manager with prior approval by the DAAC management at a time that minimizes disruption to system users, usually during off hours. No loss of data is anticipated from a normal shutdown. All subsystems are shutdown in a routine and normal fashion.

The system shutdown procedure is performed by the System Administrator at the discretion of the Network Administrator, usually for the purpose of repair. The system shutdown is normally performed in reverse order of the system startup. Figure 2 below shows the order at the DAAC in which each server is to be shutdown to achieve an orderly shutdown.

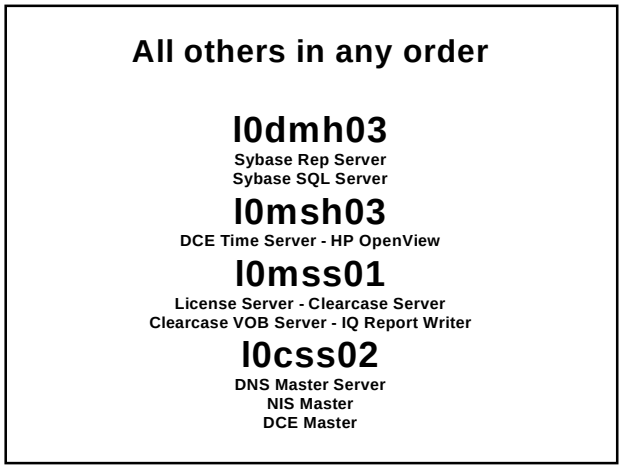

Figure 2. DAAC Server Shutdown Order

The System Administrator must be logged in as root to perform a shutdown.

Prior to a normal shutdown, the System Administrator sends broadcast messages to all Computer Operators on the system at Shutdown Minus 30 minutes, Shutdown Minus 15 minutes, and

Shutdown Minus 1 minute. At the scheduled shutdown time, the System Administrator blocks all incoming requests from the gateway and allows active jobs to complete (unless it is anticipated that they will take longer than 10 minutes in which case the System Administrator will terminate the processes and notify the originator). The System Administrator then begins to shut down all subsystems the order prescribed in the procedure below.

HP OpenView is used as the monitoring agent with each subsystem icon turning red as it is successfully shutdown. When all subsystems have been successfully shutdown, the UNIX prompt appears on the console screen. Total time from shutdown initiation to completion may be as long as 45 minutes.

Normal Shutdown By Subsystem Procedure

Steps A-G below are preliminary steps to shutting down each subsystem.

A Login to the server as **root**.

B Enter root password.

C Type **wall** and press **Return**.

D Type **This machine is being shutdown for *reason*. Please save your work and log off now. We are sorry for the inconvenience.** Press Control and D keys simultaneously.

E Wait at least five minutes.

F Type **shutdown -g0 -i0** or **shutdown now -i0** at the UNIX prompt and press **Return**.

G Power off all peripherals and the CPU.

1 Determine which machines perform the following functions:

- DNS Master
- NIS Master
- Mail Hub Server(s)
- Automount Server
- Clearcase Server
- CSS including DCE Server
- DCE License Server for SUN
- Other License Servers
- MSS including Tivoli Server and Sybase SQL Servers
- DSS
- Ingest
- PDPS
- CIDM

2 Power off the CIDM server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 3.

3 Power off the PDPS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 4.

4 Power off the Ingest server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 5.

5 Power off the DSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 6.

6 Power off the MSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 7.

7 Power off the Other License server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 8.

8 Power off the DCE License server for the SUN by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 9.

9 Power off the CSS server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 10.

10 Power off the Clearcase server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 11.

11 Power off the Automount server(s) by following steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to step 12.

12 Power off the Mail Hub server(s) by following steps A-G above for each machine. Once the system has shutdown without error, proceed to step 13.

13 Power off the NIS Master by following steps A-G above for each machine. Once the system has shutdown without error, proceed to step 14.

14 Power off the DNS Master.

Emergency Shutdown

An emergency shutdown is indicated when the System Administrator determines that the entire system or a component subsystem requires immediate maintenance. Indications that an emergency shutdown is in order include:

- the system or subsystem is locked up and users are unable to access or maneuver through the system
- an impending or actual power failure
- an actual system or subsystem hardware or software failure

Every effort should be made to minimize loss of data during an emergency shutdown by informing users to save files and log off if at all possible. However, circumstances may be such that a large-scale loss of data is unavoidable. In such instances, data will be restored from the most recent backup tapes and temporary backup files provided by the system (if applicable).

If the entire system is locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If major subsystems are locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If one or only a few of the subsystems are experiencing problems and only some of the users are impacted, the subsystem problem(s) should be resolved first. If after all efforts to resolve the subsystem problems are exhausted the System Administrator determines that a shutdown is necessary, only those affected subsystems should be shutdown. Only if these steps provide no relief should the entire system be brought down. In any case, every effort should be made not to impact users that are still on the system and to minimize data loss.

Emergency Shutdown Procedure

1 Login to the server as root.

2 Enter root password.

3 Type **sync** at the UNIX prompt, then press **Return**.

- **sync** causes all information in memory that should be on disk to be written out including modified super blocks, modified inodes, and delayed block I/O. If the system is to be stopped, sync must be called to insure file system integrity.

4 Type **sync** again at the UNIX prompt, then press **Return**.

5 Type **halt** at the UNIX prompt, then press **Return**.

6 Shutdown all client workstations.

7 Determine which machines perform the following functions. Some machines may perform multiple functions:

- Sybase SQL/Rep
- Autosys
- Clearcase
- Tivoli
- DCE
- Automount
- Mail Hub
- NIS
- DNS

8 Power off the Sybase SQL/Rep server(s). Once the system has shutdown without error, proceed to Step 9.

9 Power off the Autosys server(s). Once the system has shutdown without error, proceed to Step 10.

10 Power off the Clearcase server(s). Once the system has shutdown without error, proceed to Step 11.

11 Power off the Tivoli server(s). Once the system has shutdown without error, proceed to Step 12.

12 Power off the DCE server(s). Once the system has shutdown without error, proceed to Step 13.

13 Power off the Automount server(s). Once the system has shutdown without error, proceed to Step 14.

14 Power off the NIS server(s). Once the system has shutdown without error, proceed to Step 15.

15 Power off the DNS server(s).

In case of EXTREME emergency where time does not allow you to execute the above procedures, execute the procedure steps that follow. Be forewarned, however, that this procedure does not ensure file system integrity and will result in loss of data and/or damage to the file system. It should be used only as a last resort.

Extreme Emergency System Shutdown Procedure

---

1 At the **Login:** prompt, type **root,** then press **Return**.

2 At the **Password:** prompt, enter the ***RootPassword***.

3 Press the **L1** and the **a** keys simultaneously.

4 Once returned to an **ok** or > prompt, turn the power switches on the CPU and all peripherals to the **off** position.

WARNING

The use of L1-a does not ensure file system integrity. There is a very high risk of losing data when this process is used.

System Shutdown by Server

In situations where only a single server requires maintenance the System Administrator will need to determine if and how the faulty server affects other servers on the network. One server may be able to be shutdown without affecting the rest of the network, or several dependent servers may have to be shutdown in addition to the target server. Because of these interdependencies, each case will have to be uniquely evaluated.

The ECS Assistant

What is ECS Assistant?

ECS (EOSDIS Core System) is a complex system comprising many subsystems and components running on multiple heterogeneous host machines. The coordination of all the subsystems is an arduous, time consuming, error prone task. In order to improve our effectiveness and efficiency, an easy-to-use GUI tool, "ECS Assistant," has been developed to facilitate ECS Maintenance activities.

Currently, the ECS Assistant is comprised of three major scripts: EcCoAssist, EcCoModemgr, and EcCoEsdtmgr. These scripts provide users with a Graphical User Interface to perform functions such as subsystem server startup and shutdown, ESDT management, and database review when using the ECS system. During the course of performing their tasks, operators can use ECS Assistant to perform the following functions through its GUI:

- To start up and shut down servers for each subsystem
- To graphically monitor the server up/down status
- To open and view the detailed log files for each server used
- To review various databases used in the ECS system

In the following sections, we will address aspects of how to use the ECS Assistant. Section one explains how to use ECS Assistant to facilitate and manage the subsystems and their servers, including server start up and shut down. Section two describes how to monitor servers for each subsystem, including using the ECS Monitor and ECS logfile viewer.

Using ECS Assistant to Start Up / Shut Down Servers

This procedure describes routings for using the ECS Assistant GUI to start up and shut down subsystem servers. The procedure described here will apply to all the servers from different subsystems. The next procedure will describe how to monitor the servers' status with the ECS Assistant.

Detailed procedures for tasks performed by the System Administrator are provided in the sections that follow.

Assumptions:

1. The ECS Assistant has been properly installed.
2. The required environment variables have been set properly.

To run the ECS Assistant, execute the procedure steps that follow:

Subsystem Server Start Up / Shut Down Procedure

1 Log into one of the host machines.

2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv DISPLAY *hostname*:0.0**, press **Return**.

- The ***hostname*** is the name of the machine on which the ECS Assistant is to be displayed, *i.e.,* the machine that your are using.
- To verify the setting, type **echo $DISPLAY**, press **Return**.

3 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs**, press **Return**.

- To verify the setting, type **echo $ECS_HOME**, press **Return**.

4 If necessary, at the UNIX prompt on the host from which the ECS Assistant is to be run, type **cleartool setview *ViewName***, press **Return.**

- The ***ViewName*** is the ClearCase view to be used while the ECS Assistant is running in this session. For example, type **cleartool jdoe**, press **Return**.
- A ClearCase view is required only if the ECS Assistant needs to be able to "see" into a ClearCase VOB; a view is not necessary otherwise.

5 At the UNIX prompt, type **cd /tools/common/ea**, press **Return**. Then type **EcCoAssist &**, press **Return**.

- **/tools/common/ea** is the path where ECS Assistant is installed.

This will invoke the ECS Assistant GUI with three push buttons for selecting the proper activities, as indicated in Figure 3.

Figure 3. ECS Assistant GUI

6 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.

- This will invoke the Subsystem Manager GUI, as indicated in Figure 4.

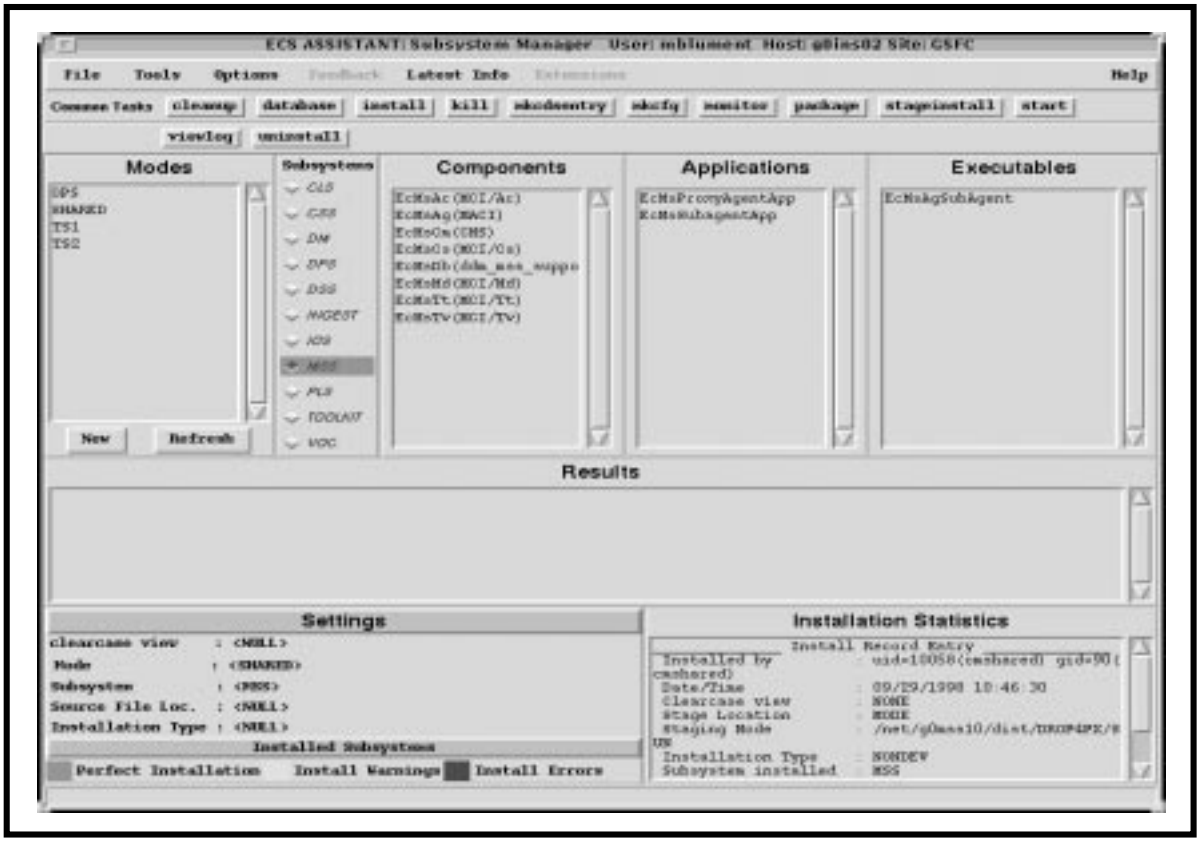

Figure 4. Subsystem Manager GUI

7 Select a mode by clicking a mode in the mode listing.

- Once the mode is selected, the color of the subsystem name list is changed.

8 Select a subsystem with the **Subsystem** radio button.

- The component list for the selected subsystem will appear in the component window.

9 Select a component by clicking the component name under the component window.

- The selected component will be highlighted.
- The server list corresponding to that component will appear in the server window.

10 Select a server by clicking the server name from the server list under the servers window.

- The server selected is highlighted.

11 To start a server up or shut it down:

- Click the **start** button in the common tasks bar. This will start up the selected server.
- Click the **kill** button in the common tasks bar. This will shut down the selected server.

12 Repeat steps 7-11 to start up or shut down other servers.

13 To exit the Subsystem Manager GUI, select **File..Exit** in the menu bar of the Subsystem Manager GUI.

- This will terminate the Subsystem Manager GUI**.**

Note: While ECS Assistant is currently being used for system installation and server activation/deactivation, the primary tool for server activation/deactivation is HP OpenView, addressed later in this document.

Using ECS to Perform System Monitoring

ECS Assistant provides two ways to monitor server status. The first one is by performing "tail -f" to log files which record the important activity history performed on the servers. The other way is by using a database table to display server up/down status' dynamically. These monitoring methods are described in the following sections.

Using ECS Assistant to Open / View Log Files for a Selected Server

Log files are used extensively in the ECS system to record a history of activity performed on the system. They provide useful information about server activities. ECS Assistant provides an easy way to access and view these log files. In the Subsystem Manager GUI, there is one button called **viewlog** in the Common Tasks bar. Click this button to invoke a log file GUI. You can review the log files for a particular server by choosing the server name from the Menu for the Subsystem to which it belongs. You can also view all of the log files for a component by choosing it in the Components menu. Menu entries are dimmed if no log files are present. The following example shows how to use this GUI to open log files for a particular server.

Detailed procedures for tasks performed by the operator are provided in the sections that follow.

Assumptions:

1. The ECS Assistant has been properly installed.
2. The ECS Subsystem manager has been invoked.

To run the Log Viewer, execute the procedure steps that follow:

1 Click the **viewlog** button in the Subsystem Manager GUI.

- This will invoke the log viewer GUI.

2 To open and view log files for a particular server, select a server from the Subsystem pull down menu, then click the server name.

- This will open all the log files corresponding to that server.
- The log file name is indicated in the title bar for each log file GUI.

3 The log file GUI provides the following options for users to view log file contents. Follow the guidance in the GUI to select the proper options:

- **Foreground color** for changing the foreground color.
- **Background** color for changing the background color.
- **Font size** for changing font sizes.
- **View entire file** for displaying the entire file.
- **Continuous update (tail -f)** for displaying the updated log file continuously.
- **Search for** for performing word searches in the log file.
- **Print** for printing the log file.

4 To view log files for other servers, repeat steps1-3.

5 Exit the log file by pressing **EXIT**.

Using ECS Assistant to Monitor Server Status

ECS Assistant provides another convenient way to monitor the status of the servers by listing their up/down condition. The status flag for a server is up or down indicating whether or not that server is running.

Detailed procedures for tasks performed by the operator are provided in the sections that follow.

Assumptions:

1. The ECS Assistant has been properly installed.
2. The ECS Subsystem Manager is running.

To start up the ECS monitor GUI, execute the procedure steps that follow:

1 At the ECS **Subsystem Manager** GUI, select a mode by clicking a mode in the mode list.

- Once the mode is selected, the color of the subsystem name list is changed.

2 Select a subsystem by clicking the radio button next to the subsystem name under the subsystem component window.

- The selected subsystem radio button will be highlighted.
- The components corresponding to that the subsystem will be displayed in the component window.

3 Select a component by clicking its name under the component window.

- All of the applications for the selected component will be displayed in the applications window.

4 If desired, click the **monitor** button from the common tasks window.

- This will invoke the ECS Monitor GUI window as shown in Figure 5.
- The status “UP/DOWN” indicates whether or not if the server is running.

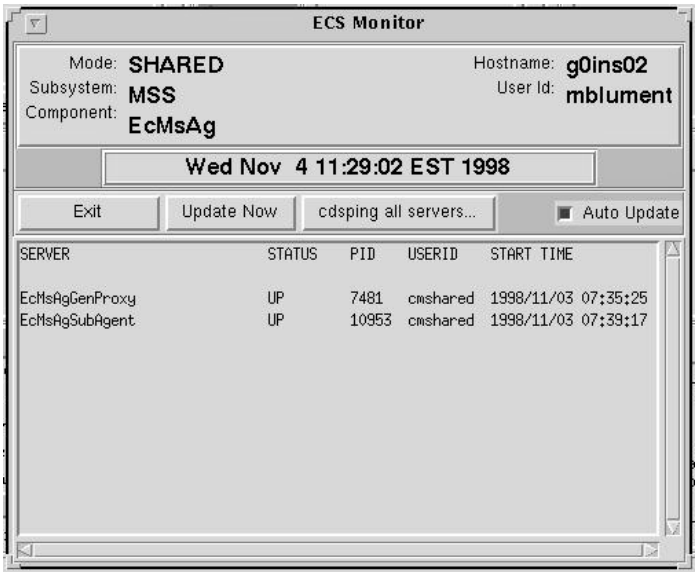

Figure 5. Server Monitor GUI

5 To see which host each server is running on, click the **cdsping all servers…** button.

- This will invoke the ECS Monitor (cdsping) GUI as indicated in Figure 6.
- The host name for each running server is listed

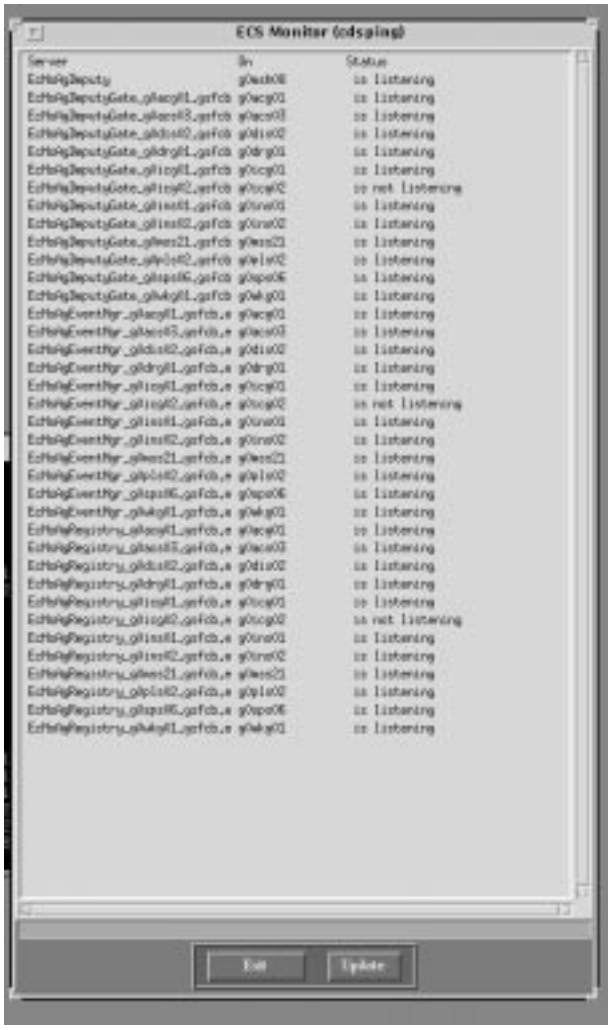

Figure 6. cdsping GUI

6 Both ECS monitor GUI and ECS Monitor (cdsping) GUI can be updated by clicking the **update** button in the GUI.

- This will cause the list to update to the current status.

7 To monitor other servers, repeat steps 2-4.

8 To exit, click the **EXIT** button.

- This will end the monitor GUI.

This page intentionally left blank.

HP OpenView - Network Node Manager

What is HP OpenView?

ECS is heavily dependent on the use of computer networks and their complexity requires a comprehensive monitoring agent to assist you in system management. Hewlett-Packard OpenView (HPOV) Network Node Manager (NNM) is just such an agent. It is a multi-vendor network management tool that, among other things, provides system administrators with a means to bring up and take down ECS servers and monitor their status. This can be accomplished either at an overall Mode level (i.e., TS1, TS2, or OPS) or individual System level (i.e., MSS, IDG, etc.). It also is a powerful management tool that is capable of providing:

- dynamic discovery and updating of network topology including IP hosts, gateways, and networks.
- a site-wide view of network and system resources.
- status information on resources.
- event notifications and background information.
- operator interface for managing resources.

Network Node Management functions are addressed in detail in the Network Administration lesson, Volume 4. This lesson will address starting and shutting down ECS Servers using HP OpenView.

Starting and Ending a NNM Session

Start NNM

In order for the NNM to properly report on the network topography, HP OpenView Windows (OVW) must be activated. Once activated, OVW automatically starts NNM. OVW also automatically starts the applications that are installed and registered.

Prerequisites for this Task

The network management processes that work with OVW and NNM must be running. The network management processes consist of the following HP OpenView background processes, among others:

- **ovwdb** - The process that maintains the OVW object database.
- **trapd -** The process that multiplexes and logs SNMP traps.
- **ovtopmd** - The process that maintains the network topology database.
- **ovactiond -** The process that executes commands upon receipt of an event.

- **snmpCollect** - The process that collects MIB data and performs threshold monitoring.
- **netmon** - The process that polls SNMP agents to initially discover network topology and then detect topology, configuration, and status changes in the network.

You can check to see if these processes are running by typing **/usr/ecs/<*mode*>/COTS/OV/bin/ovstatus**, where **<*mode*>** is normally **OPS**, **TS1**, or **TS2**.

```
object manager name: ovwdb
behavior:        OVs_WELL_BEHAVED
state:           RUNNING
PID:             174
last message:    Initialization complete.
exit status:     -

object manager name: snmpCollect
behavior:        OVs_WELL_BEHAVED
state:           RUNNING
PID:             187
last message:    Initialization complete.
exit status:     -

object manager name: ovtopmd
behavior:        OVs_WELL_BEHAVED
```

Figure 7. Sample output of* ovstatus *command

Start the HP OpenView Windows Graphical User Interface Procedure

1 Log on at workstation ***x*0msh##**.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the **##** will be an identifying two-digit number (e.g., **g0msh08** indicates a management services subsystem *hp* workstation at GSFC). If you access the workstation through a remote login (rlogin), you must enter **xhost *hostname*** prior to the rlogin, and enter **setenv DISPLAY <local_workstation IP address>:0.0** after the rlogin.

2 Type **/usr/ecs/<*mode*>/COTS/OV/bin/ovstatus** at a UNIX command prompt and then press the **Enter** key.

- A series of messages is displayed indicating for each process that its state is "**RUNNING**" or "**NOT_RUNNING**."
- If the network management processes are not running, a system administrator (logged in as **root**) can start them by typing **/usr/ecs/<*mode*>/COTS/OV/bin/ovstart**, and then pressing the **Enter** key.

3 Type **/usr/ecs/<*mode*>/COTS/OV/bin/ovw &,** and press the **Enter** key.

4 The **About OVW** box is displayed, (Figure 8) followed in a few moments by the OVW Root window, (Figure 9) and any installed and registered NNM applications are also started.

Figure 8. About OVW window

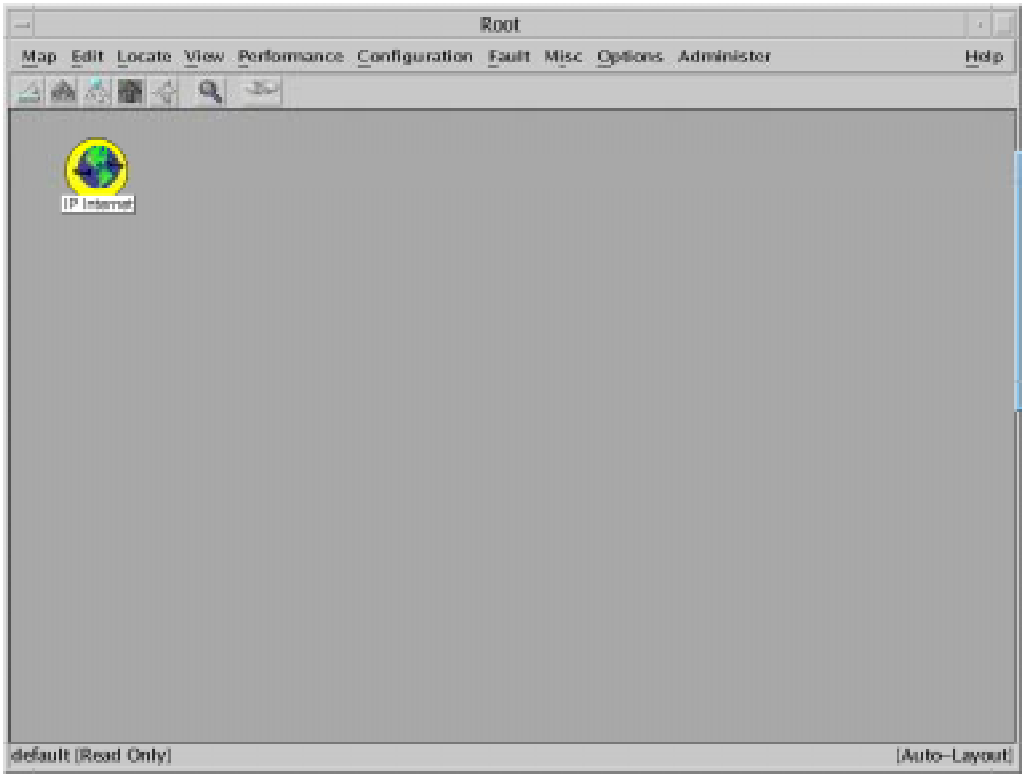

Figure 9. HPOV Root window

Exit HP OpenView Network Node Manager Session

To exit NNM and all other integrated applications, you must exit OVW in one of the following two ways:

Exit NNM Procedures

1 From the menu bar on any submap window, select **Map**, then select **Exit**; ***or***

2 Click on the **Close Map** button on all open submap windows until a warning dialog box is displayed. Then click on the **Close** button to exit OVW.

> ***WARNING: Do not use the CLOSE WINDOW button in the upper left corner of the window to exit OVW. This may cause some OVW processes to remain in operation and could result in system-wide problems later.***

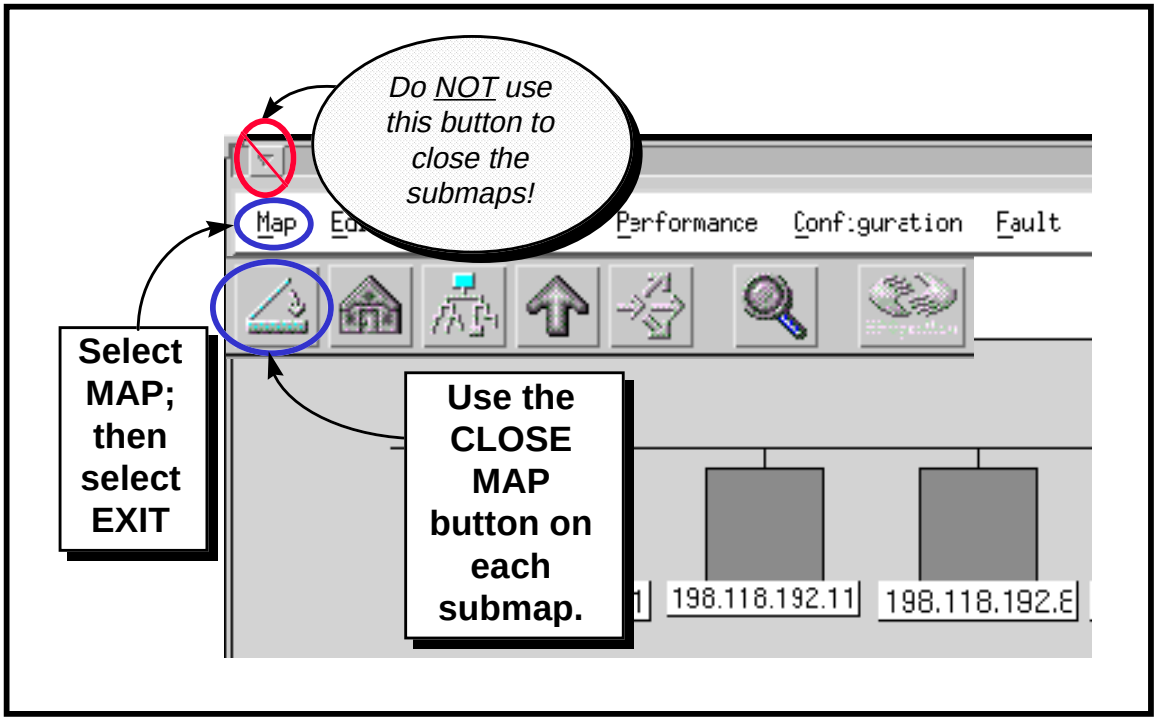

Figure 10. End a NNM Session

The NNM Submaps

The NNM Map is never seen in its entirety. What you observe when using NNM is a set of hierarchical submaps that allow you to view specific portions of the map as you track network activity.

A **MAP** is:

- A set of related objects, symbols, and submaps.
- A collection of submaps.
- Represents topology and state of real-world network.

A **SUBMAP** is:

- A collection of related symbols.
- Represents a view of the network.
- Part of the hierarchical structure

Figure 11 shows the hierarchical structure of submaps.

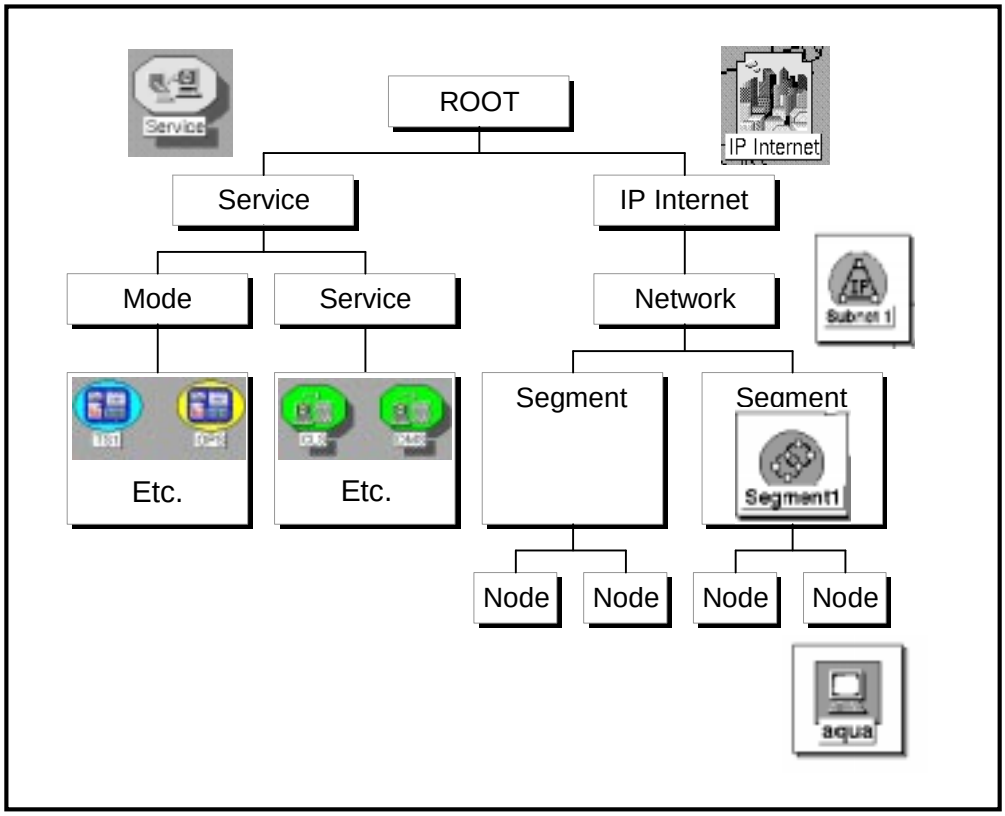

Figure 11. HP OpenView submaps hierarchy.

Figure 12 shows examples of the different levels of HP OpenView screens.

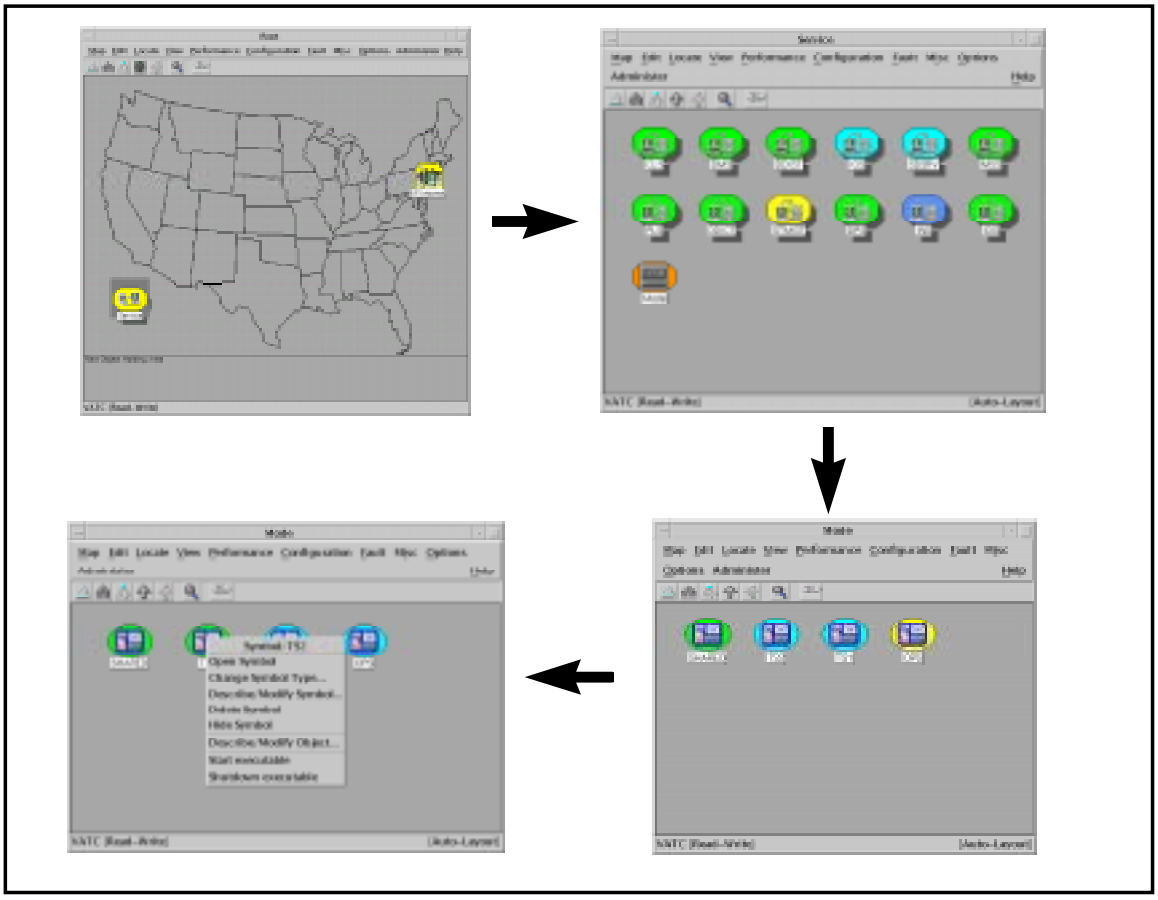

Figure 12. Submap example screens

As shown in figure 13, there are four parts to each submap:

1 Menu Bar

2 Tool Bar

3 Viewing Area

4 Status Line

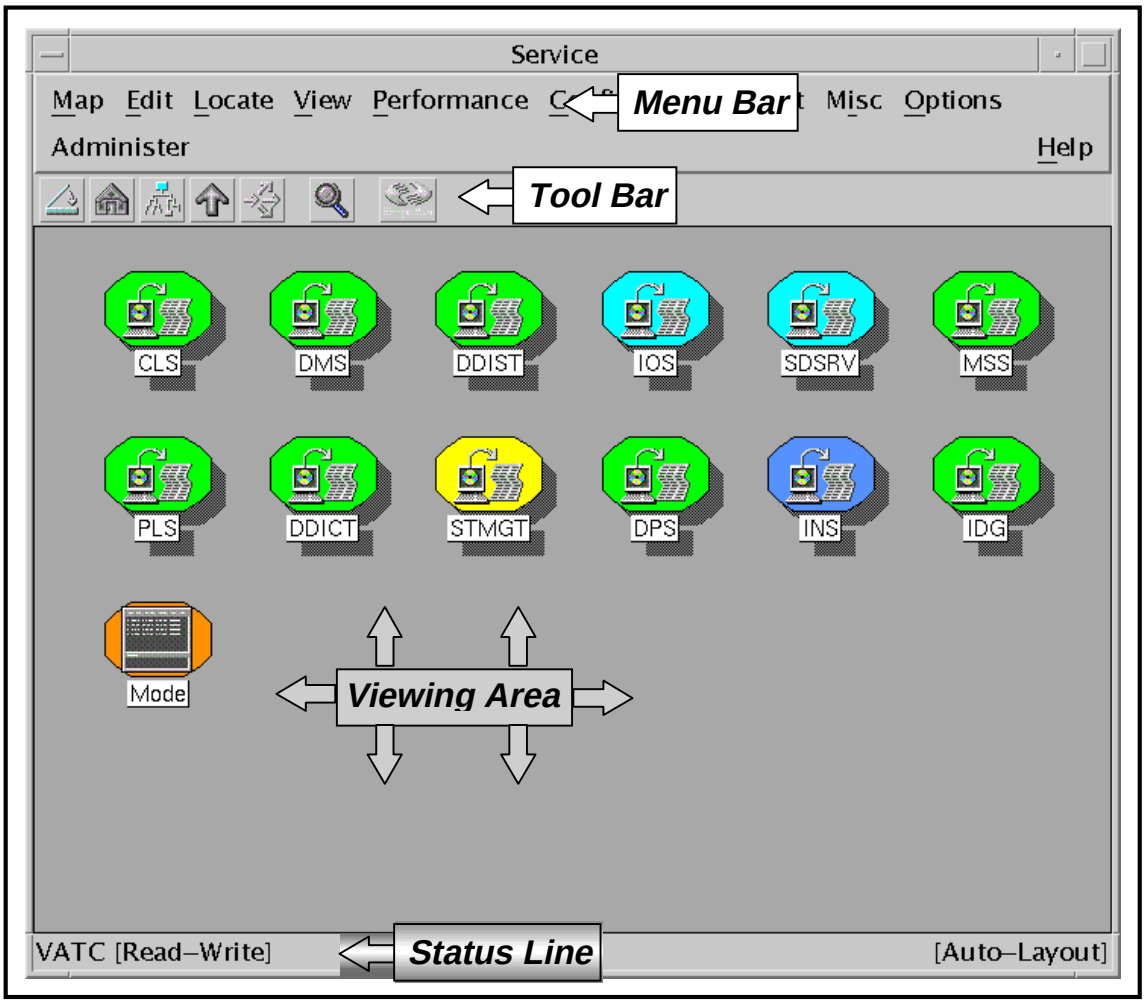

Figure 13. Parts of a Submap

Menu Bar

The **Menu Bar** offers a set of choices for performing a variety of tasks such as creating new maps and submaps, creating and modifying object information, and configuring thresholds.

Tool Bar

The **Tool Bar** (Figure 14) is used to quickly maneuver through the graphical displays. The Tool Bar has several special buttons that perform a variety of routine tasks.

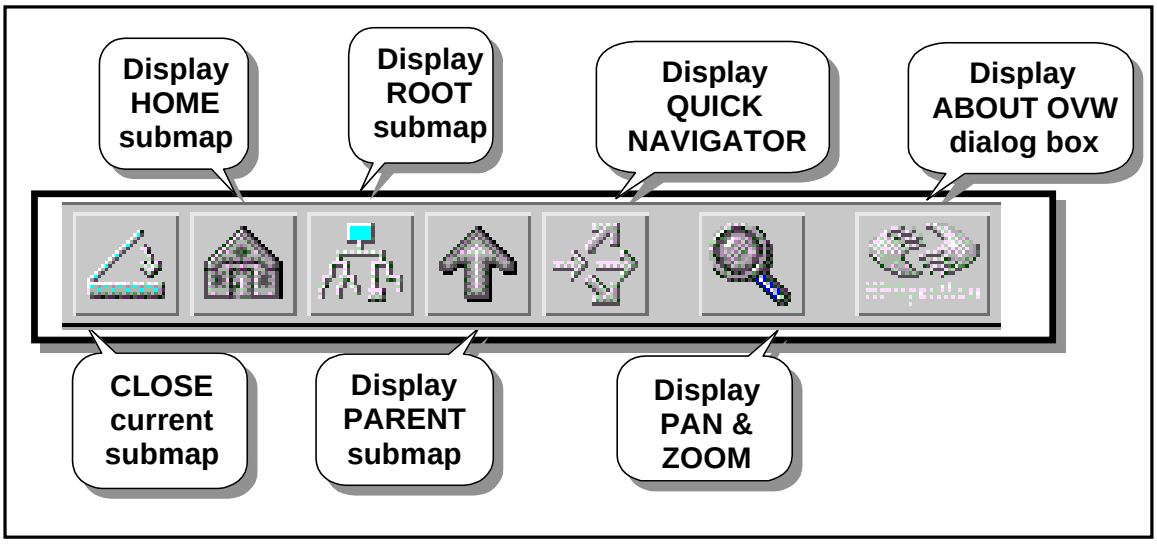

Figure 14. Sample Tool Bar

HOME button – When NNM starts up, you are placed in a particular submap by default. This default submap is called the **home** submap. Any submap can be so identified. When the **Home** button is selected, the display returns your particular home submap.

ROOT button – Displays the **root** submap.

PARENT button – Displays the **parent** submap to the current submap.

CLOSE button – Closes the current submap. Use this button to back your way out of NNM. This performs the same procedure as selecting **Map → Close Submap** from the pull-down menu.

QUICK NAVIGATOR button – Allows you to move from one submap to another without moving explicitly through the hierarchy. Using the Menu selection **Edit → Add to Quick Navigator**, you can select specific submaps or symbols that you monitor on a regular basis.

PANNER button – Some submaps are so extensive that the entire submap view cannot be seen. Using this panner allows you to shift the view of a particularly large submap so that you can zoom in on a desired area of a submap.

ABOUT OVW DIALOG button – Displays the OVW dialog box.

Viewing Area

The **Viewing Area** is your window into the submap being currently displayed. By default, the entire submap is shown within the viewing area. On some complex maps you may wish to use the **Pan and Zoom** feature to zero in on a specific area.

Status Line

Messages on the status line indicate the status of OVW including:

the name of the open map.

Read-Write access permissions.

name of the open submap.

status of the auto-layout feature (on or off).

Other messages may appear on the Status Line from time to time, such as synchronizing, which indicates that the map is being updated with the latest information in the MIB.

Starting and Shutting Down Servers from HP OpenView

One of the key features of HP OpenView is its capability to start and shutdown system servers using the graphical user interface. This can be accomplished either for all servers in a specific mode or individually by subsystem. Using this procedure will save significant effort over command-line initiation of servers.

Starting and Shutting Down Servers from HP OpenView Procedure

1 Start the HP OpenView application

2 After the **About OVW** box is displayed, the OVW **Root** window, (figure 15), will appear. From the menu bar click on the **Map; Maps; Open/List** selections (figure 16) to bring up the **Available Maps** selection window (figure 17).

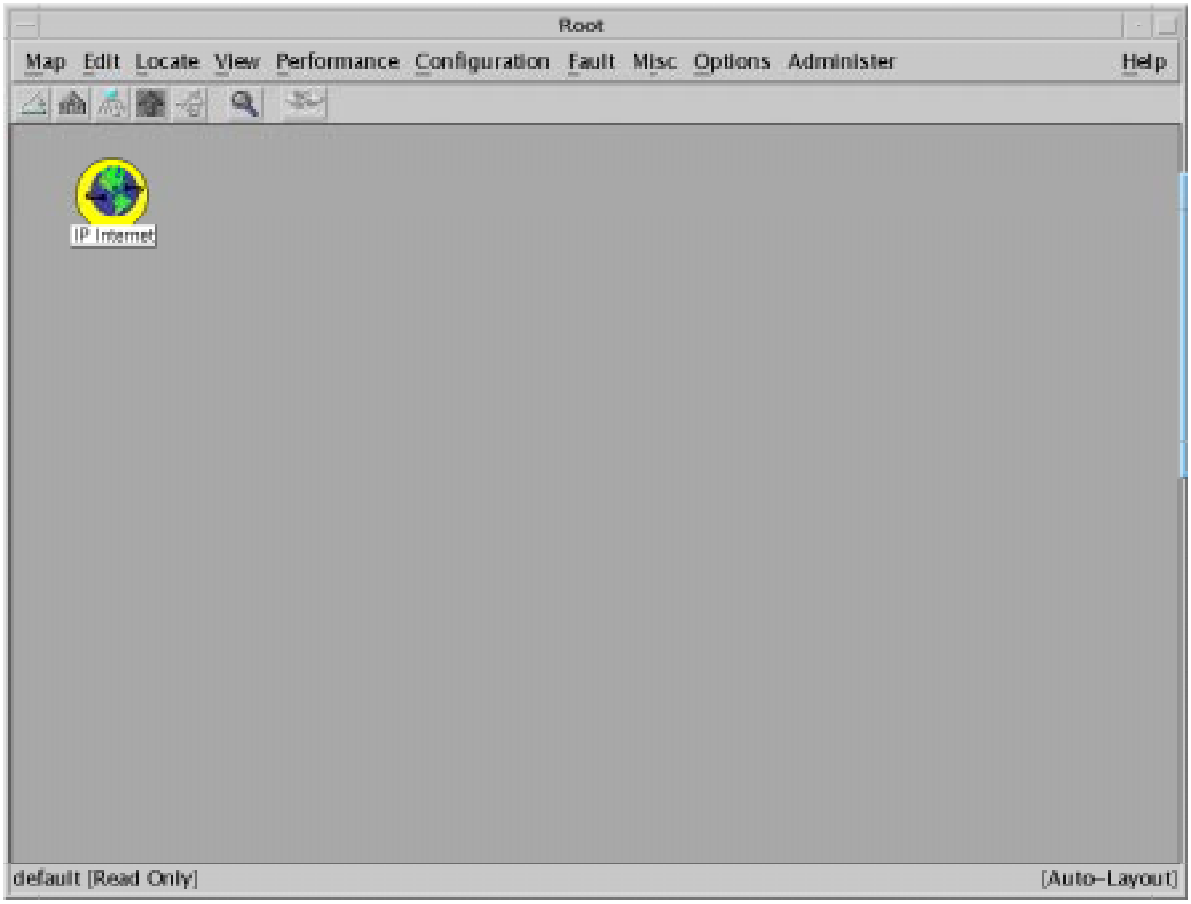

Figure 15. HPOV Root window

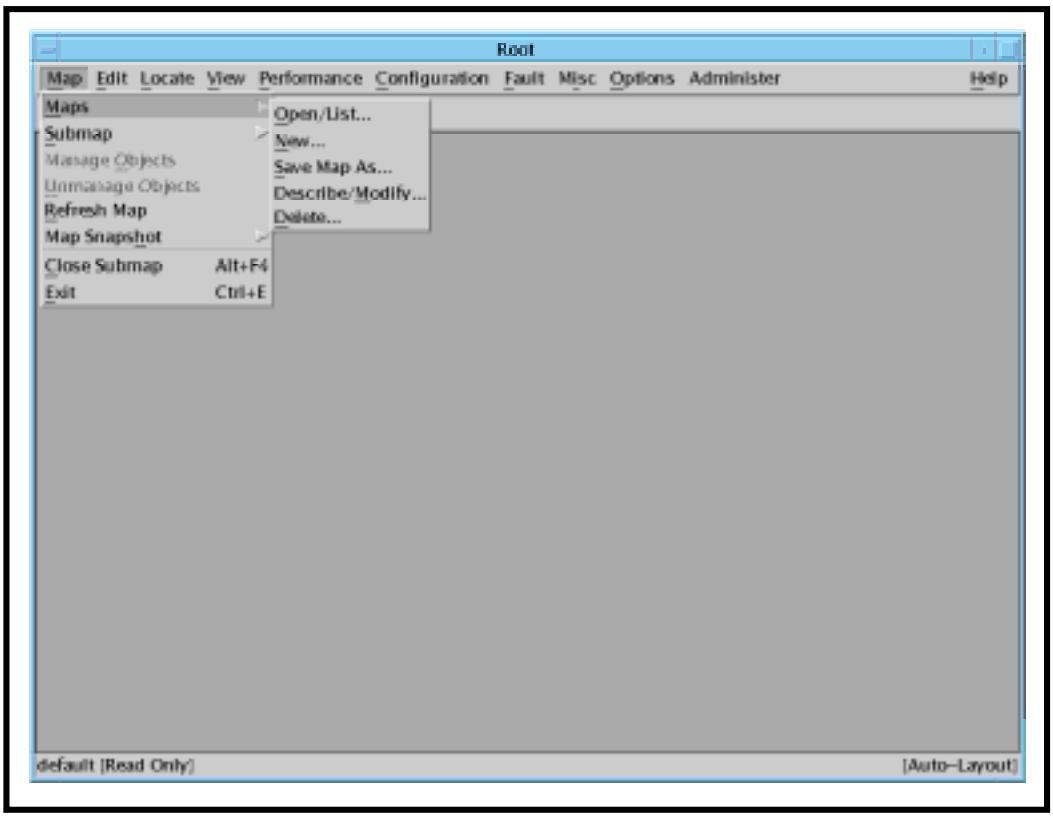

Figure 16. Maps select window

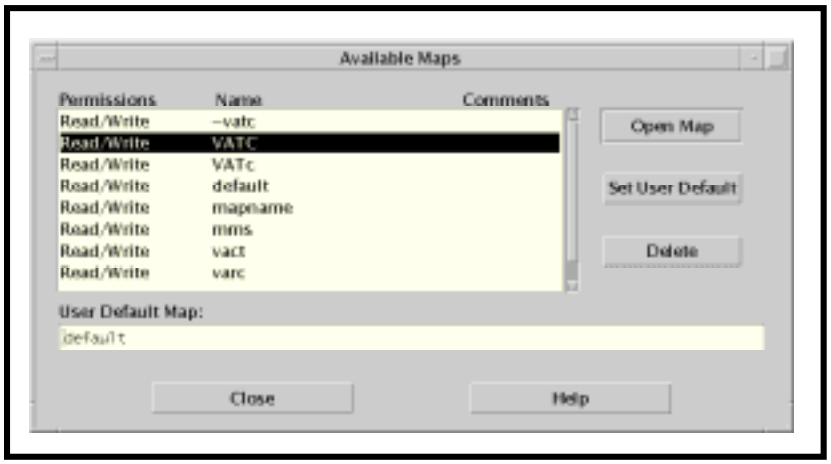

Figure 17. Available Maps window

3 Select the desired map to bring up the **Root** map that displays the **Services** and **IP Internet** icons (figure 18). Double click on the **Services** icon to display the **Service** submap.

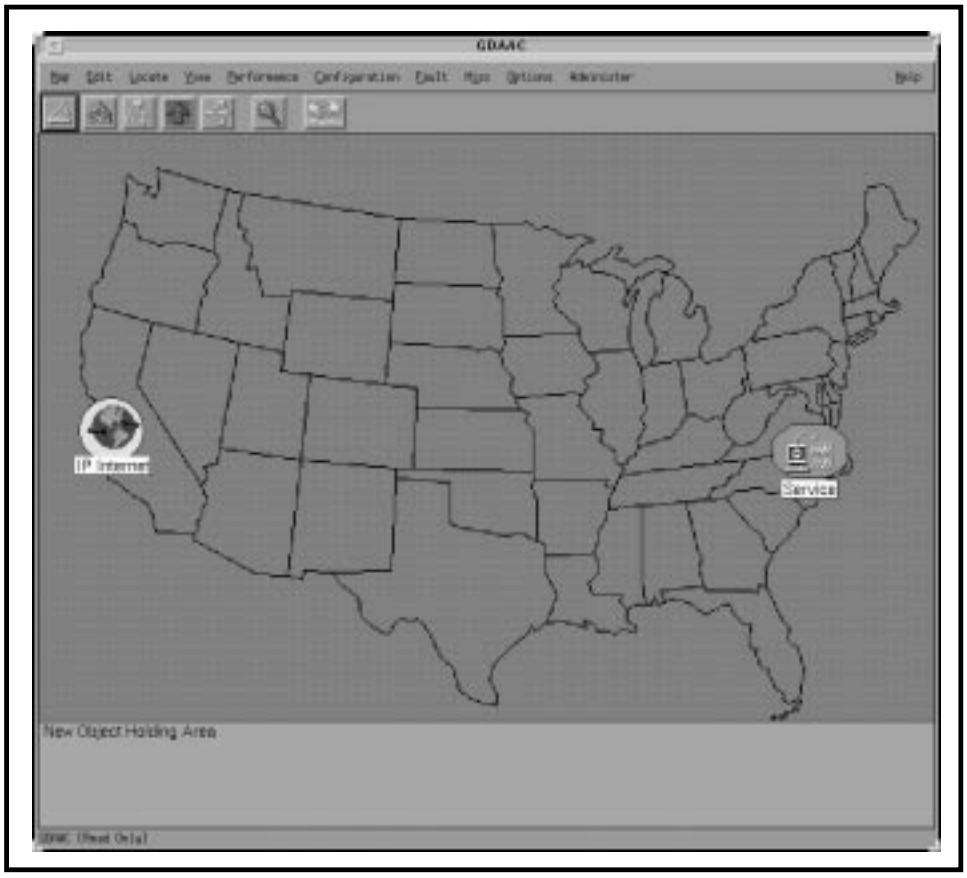

Figure 18. Root map

4 From the **Service** submap, Figure 19, select either the **Mode** icon to bring up the Mode submap (figure 20) to start or shutdown all servers for a given mode (TS1, TS2, OPS, etc.), or select a specific subsystem icon to start or shutdown servers for a specific subsystem. (go to step 6)

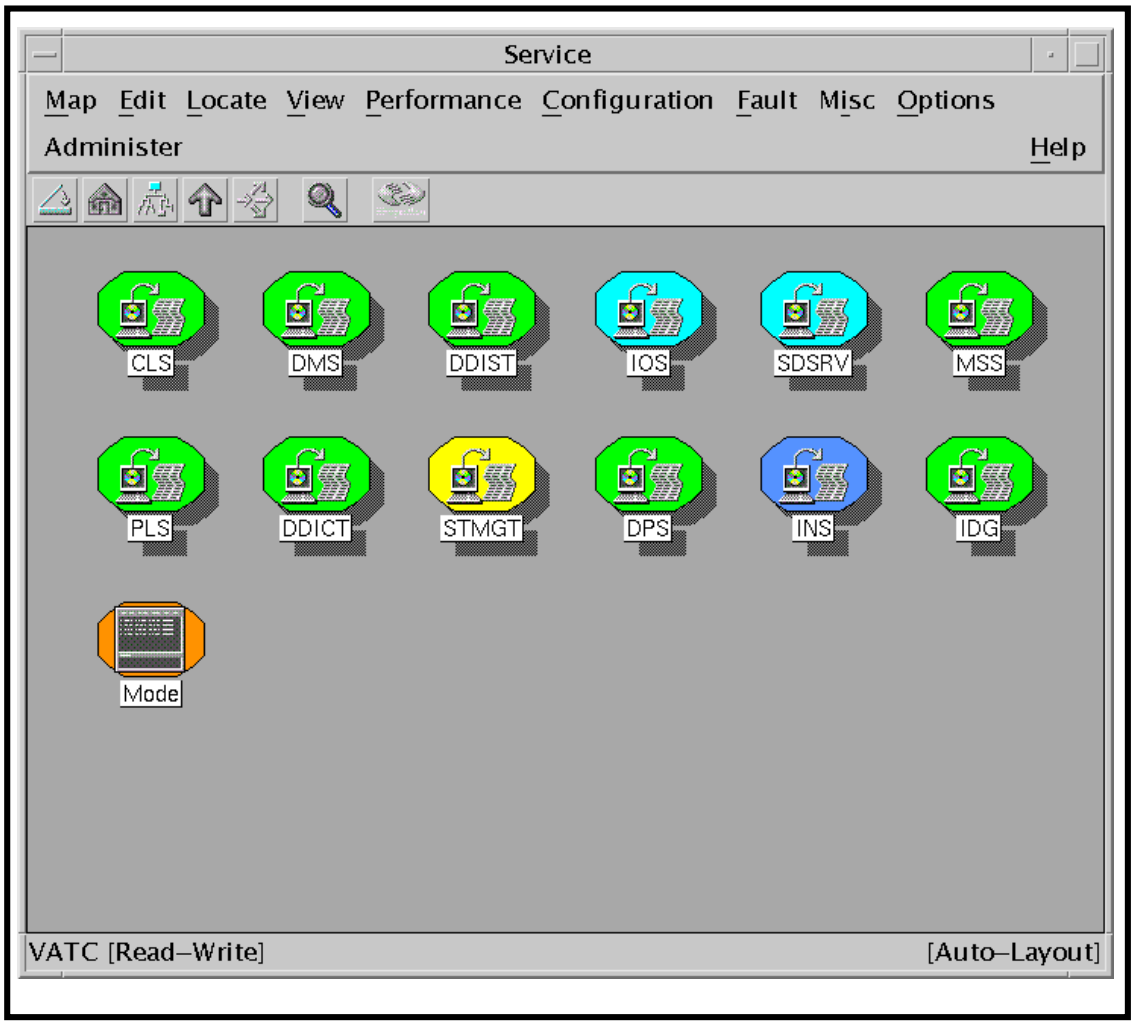

Figure 19. Service submap

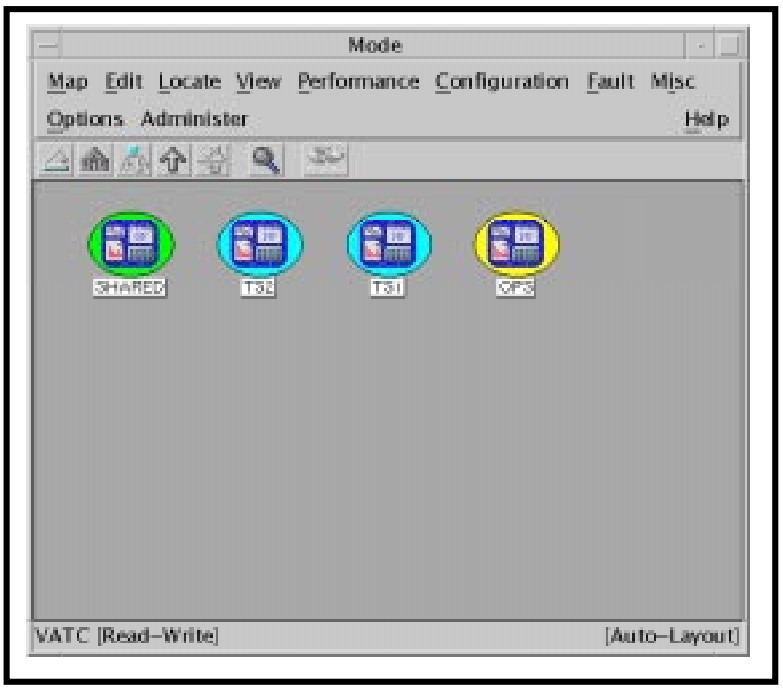

Figure 20. Mode submap

5 Right-click and hold on the desired Mode icon to display the pop-up menu shown in Figure 21, continue to hold and scroll down to either the **Start executable** or **Shutdown executable** option. Release the right mouse button and the servers for the selected mode will start or shutdown.

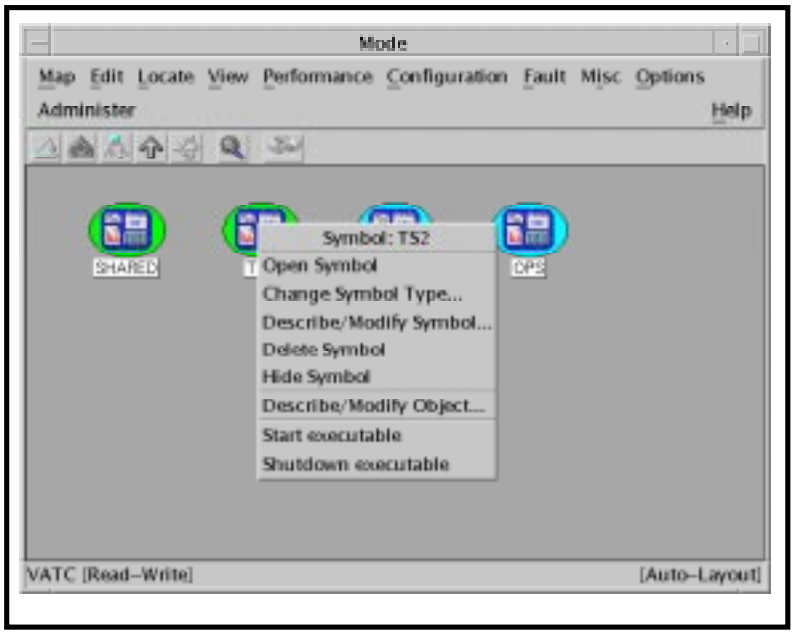

Figure 21. Start/Shutdown executable pop-up menu

6 To start or shutdown specific servers in a subsystem (CLS, MSS, IDG, etc.), double-click on the desired subsystem icon in the **Service** submap. (Figure 19).

7 From the expanded submap, Figure 22, right-click and hold on the desired server application to display the pop-up menu, scroll down to the **Start executable** or **Stop executable** option, release the button and the server will start or shutdown.

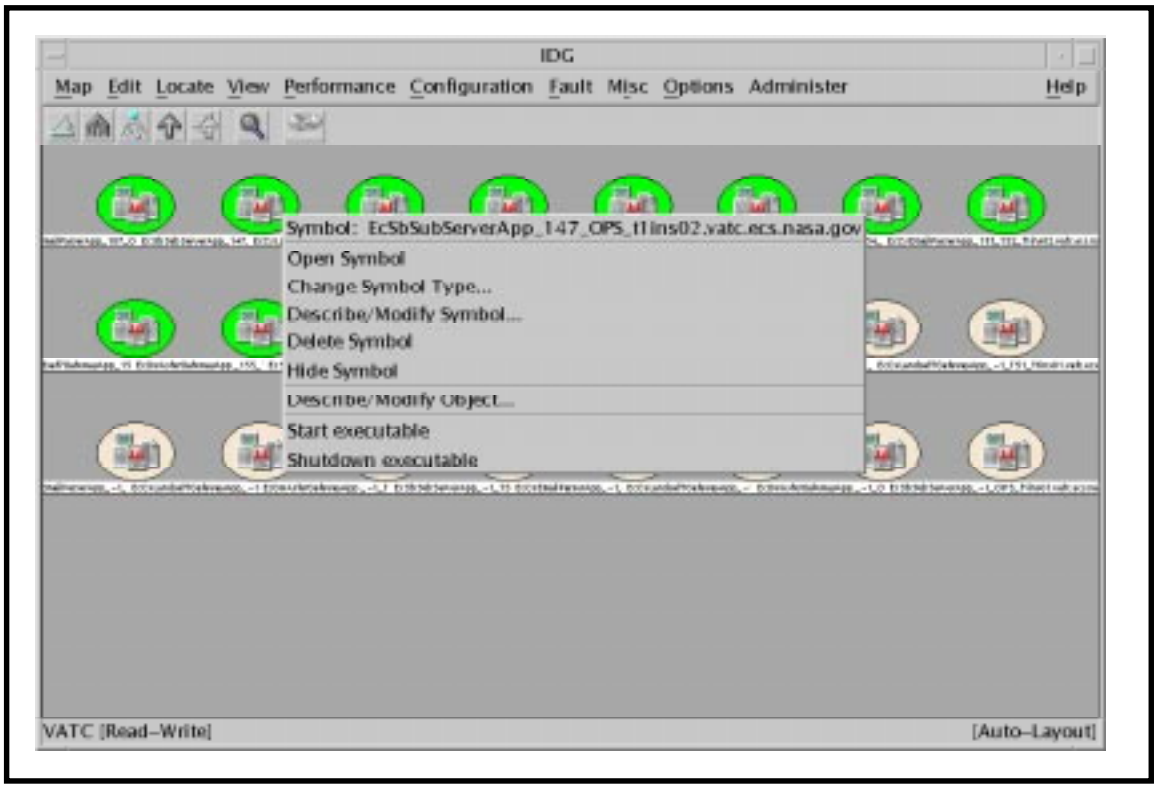

Figure 22. Subsystem submap pop-up window

This page intentionally left blank.

Secure Shell (ssh)

In this lesson you will learn how Secure Shell is used to make the ECS working environment more secure by using the Secure Shell (**ssh**) and Secure Login (**slogin**) commands to access ECS systems.

What is Secure Shell?

Secure Shell (ssh) is a set of programs that greatly improve network security. The primary need for it on ECS is to allow secure, interactive access to ECS DAACs without needing burdensome procedures and mechanisms and additional hardware.

Secure in this context means not sending passwords "in the clear" so that intruders may intercept them and also encryption of the entire session.

Secure Access to ECS DAACs

ECS has implemented a Local Area Network (LAN) at the DAACs that is more secure than most other LANs. From the Internet, it is not possible to directly connect with all hosts at a DAAC. There are a set of hosts that are "dual-homed" to a user LAN that is connected on one side to the Internet and to the DAAC production LAN on the other side. This will require an interactive user to first ssh to a dual homed host and then ssh to a production host. In order to minimize the impact on the user, a single login has been implemented.

The ECS LAN design also ensures a connection in one direction will be possible but going the other way will not. In Landover, for instance, a connection can be made from the EDF (or the MiniDAAC) to the VATC but not the other way from the VATC to the MiniDAAC due to the Raytheon firewall.

Setting Up ssh

Ssh programs have client and server components much like other network programs. The user only needs to be concerned with the client configuration as the server side is done by a systems administrator. The amount of effort that it takes to get ssh going depends on how many different home directories the user has. At Landover, for instance, there are separate directories for the EDF, the MiniDAAC and the VATC.

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. The process is started by running the sshsetup script which will enable ssh to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

Initiating sshsetup procedure

1 Login to your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell setup by typing **/tools/bin/sshsetup**, then press Return.

- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

Initializing random number generator...

Generating p: Please wait while the program completes ...

%

- This establishes the .ssh sub-directory in your <username>/home directory, creates the local ssh key, and creates the necessary files.

Remote ssh Access

If you need to access a host with a different home directory, you will need to run the sshremote script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

Setting up remote access ssh procedure

1 Login into your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell remote setup by typing **/tools/bin/sshremote**, then press Return.

- You will see the following prompt:

You have a local passphrase. Do you want to setup for:

1 VATC

2 EDF

3 MiniDAAC

4 GSFC DAAC

5 GSFC M and O

6 EDC DAAC

7 EDC M and O

8 LaRC DAAC

9 LaRC M and O

10 NSIDC DAAC

11 NSIDC M and O

12 Exit from script

Select:

3 At the "Select" prompt, type in the corresponding number to the desired host, then press Return.

- You will receive a prompt similar to the following for the VATC:

Working...

4 At the prompt "Enter passphrase for RSA key '<username>@<hostname>': Type in your **passphrase** and then press Return.

- A prompt similar to the following will be displayed:

Last login: Thu Jul 9 10:41:13 1998 from echuser.east.hit

No mail.

Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996

t1code1{username}1:

5 At the prompt "Press <ctrl>a to run sshsetup and exit <enter> to logoff t1code1u", type **<ctrl>-a** to initiate the sshsetup script on the remote host

- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces

6 At the prompt "New passphrase:" **enter your passphrase <enter>**.

7 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

Initializing random number generator...

Generating p: Please wait while the program completes ...

%

8 At the "t1code1" prompt type **exit**, the press Return.

- The following information will be displayed:

Updating locally...

Updating t1code1u.ecs.nasa.gov

%

- This establishes the ssh key at the remote host and exchanges key information with your local host.

Note: The ssh keys at remote sites can be different from the local host ssh key

Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The ssh keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

Changing Your Passphrase Procedure

1 Login to your normal Unix workstation where your home directory resides.

- Initiate passphrase change by typing **/tools/bin/sshchpass**, then press Return.
- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces

2 At the prompt "Old passphrase:" **enter your old passphrase <enter>**

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see an information prompt similar to the following:

ssh-keygen will now be executed. Please wait for the prompt to return!

/home/bpeters/.ssh/authorized_keys permissions have already been set.

%

Tape Operations

In this lesson you will learn how Networker Administrative software and the Exabyte tape drive work together to administer the use of tapes for system backups and file restorations. Functions such as how to label a new tape, how to index a tape cartridge, and how to perform backups and restores are covered.

TERMS:

- **Cartridge** - A hardware device that is part of the Exabyte tape drive. It holds up to 10 tapes that are automatically selected by Networker.
- **Drive** - Hardware device into which the tape or tape cartridge is inserted that performs the actual recording of data.
- **Index** - A list of the labeled tapes currently stored in the jukebox.
- **Inventory** - The action of making an **index**.
- **Jukebox** - A hardware device that stores more than one tape used for system backups and restores. Working in conjunction with specialized software, it can automatically select the proper tape, load the tape into the tape drive, and return it to its appropriate slot upon completion of the task.
- **Label** - A unique name assigned to a tape by Networker.
- **Volume** - A recording medium; in the case of this course, a volume and a tape a synonymous.

Networker Administrator Screen

The main Networker Administrator screen (Figure 23), which is displayed after typing **nwadmin** at a UNIX prompt, contains four main sections.

1. The menu bar at the top of the screen, which displays all of the possible capabilities of Networker Admin..
2. The **speedbar**, which can be customized, displays icons that execute the most common procedures.
3. Current configuration information, including the current Networker server, the available backup devices (tape drives, file systems, CD-ROMs, etc.).
4. Current status windows which display in real time the actual activity on the various devices, and progress and error messages.

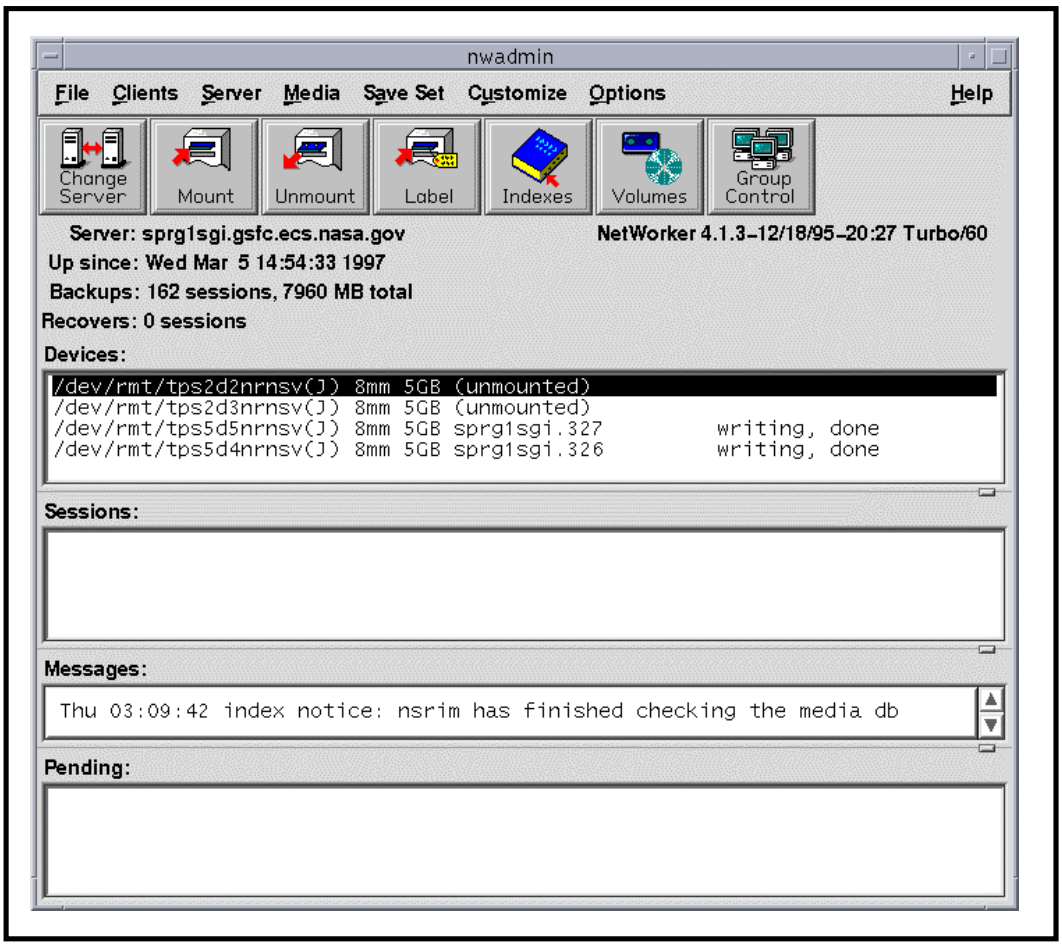

Figure 23. Networker Administrative main screen

Labeling Tapes

Files and directories have unique names that are assigned by the user to identify them. In much the same manner, tapes are given unique names, or labels. This allows such programs as Networker and such hardware devices such as the Exabyte jukebox to automate the tape selection process when performing system backups and restores. When a tape is initialized, Networker assigns it a label. Networker then stores the tape's label with a file that is written to the tape so that when a file restoration request is received, Networker will know exactly which tape to select from the jukebox.

Tape Labeling Procedure

1 Type **xhost <remote_workstation_name>** and then press the **Enter** key.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**

3 Start the log-in to the Backup client server by typing **/tools/bin/ssh *BackupServerName*** in the second window and then press the **Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing: **su**, then press **Return**.

- A password prompt is displayed.

7 Enter the ***RootPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

8 At the UNIX prompt, type **nwadmin**, then press **Return**.

- A window opens for the Networker Administrative program.

9 Insert the blank tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.

- Remove any non-blank tapes from the cartridge or else they will be re-labeled and the data on the tapes will be lost.

10 Click the **Label** button.

- The **Jukebox Labeling** window opens (Figure24).

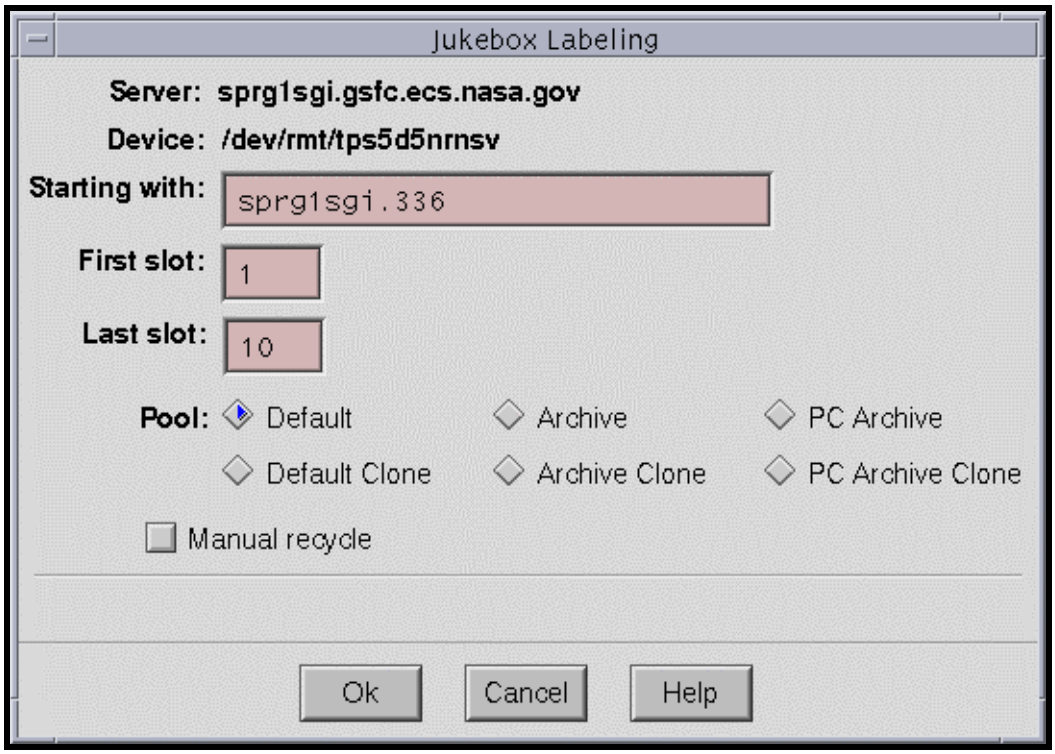

Figure 24. Jukebox Labeling window

11 In the field marked **Starting with**, enter the tape label you wish to use for the first tape in the sequence.

- Tape labels are named by using the host name (e.g., **sprn1sgi**), a dot or period, and a sequential number (e.g., **001**, **002**).
- By default, the system will prompt you with the next label in the sequence (e.g., **sprn1sgi.011**).

12 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.

- Slot 1 is at the top of the cartridge and 10 at the bottom.
- Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
- It is OK to leave empty slots.

13 Click the **OK** button.

- A status message indicating the progress of the tape labeling procedure appears and updates.
- Labeling a full cartridge of tapes takes about 15 minutes.

14 When the status in the **Jukebox Labeling** window reads **finished**, click the **Cancel** button.

- The **Jukebox Labeling** window closes.

15 From the **File** menu, select **Exit**.

- The **nwadmin** program terminates and you are returned to the UNIX prompt.

16 At the UNIX prompt for the backup server, type **exit**, then press **Return**.

- **Root** is logged out.

17 Type **exit** again, then press **Return**.

- You are logged out of and disconnected from the backup server.

18 Put an identifying sticker on the outside of each tape cassette.

Indexing Tapes

Labeled tapes are loaded in a tape cartridge that is inserted into the Exabyte tape drive, also referred to as the *jukebox.* Networker needs to know the location of each tape in the jukebox. To do this, Networker uses a process called **inventory** which prepares an index by matching a tape label to the cartridge slot that holds that tape (Figure 25). Then, when a request to recover a file or a set of files is received, *Networker* locates the tape based on the information in its memory.

CAUTION

If you move a tape from its position in the cartridge, Networker will not know where to find it (Figure 26). You must re-index the cartridge by performing these procedures again for Networker to select the correct tape (Figure 27).

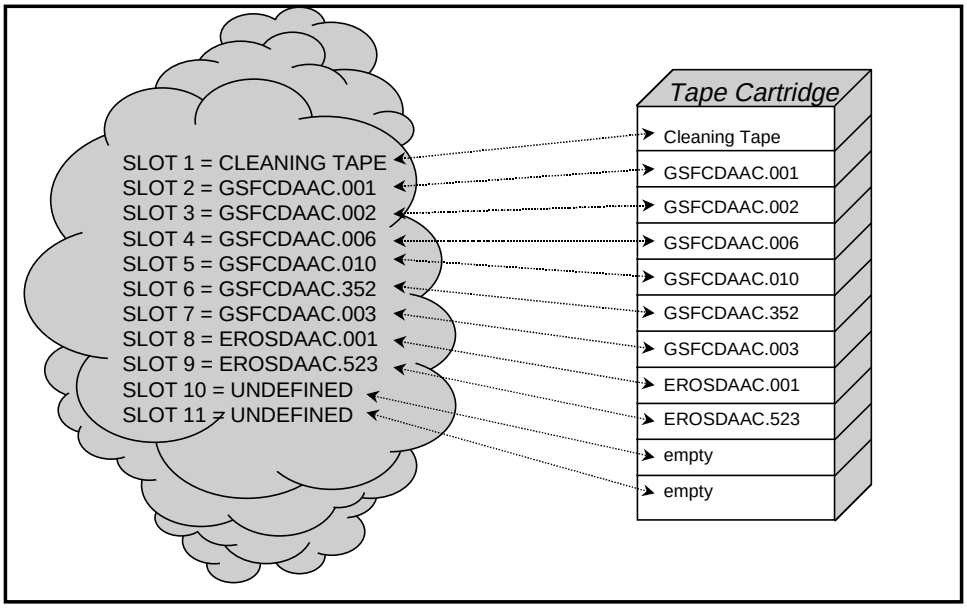

Figure 25. Tape index following the initial inventory

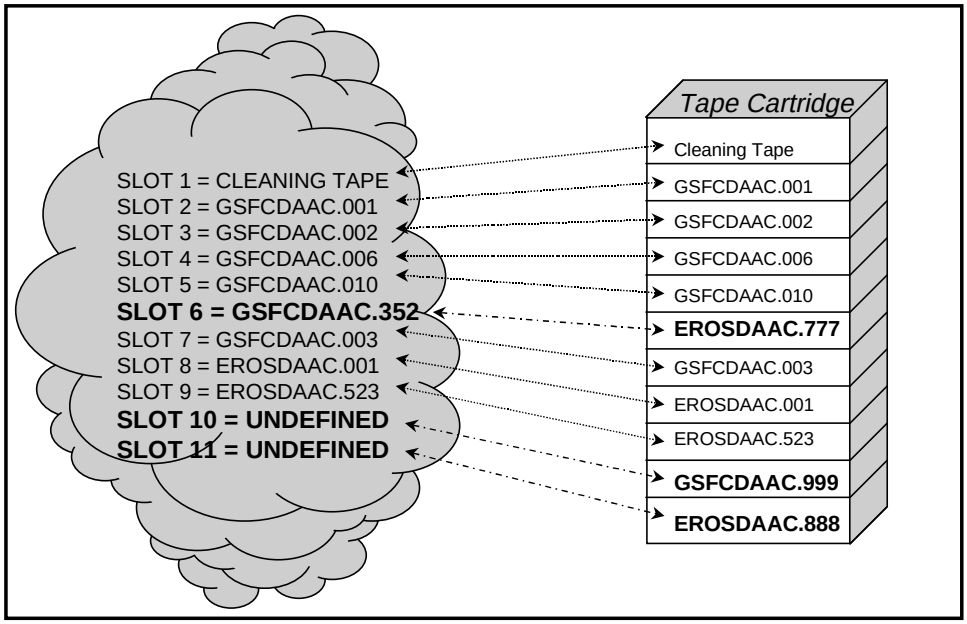

Figure 26. Tapes changed but not re-inventoried

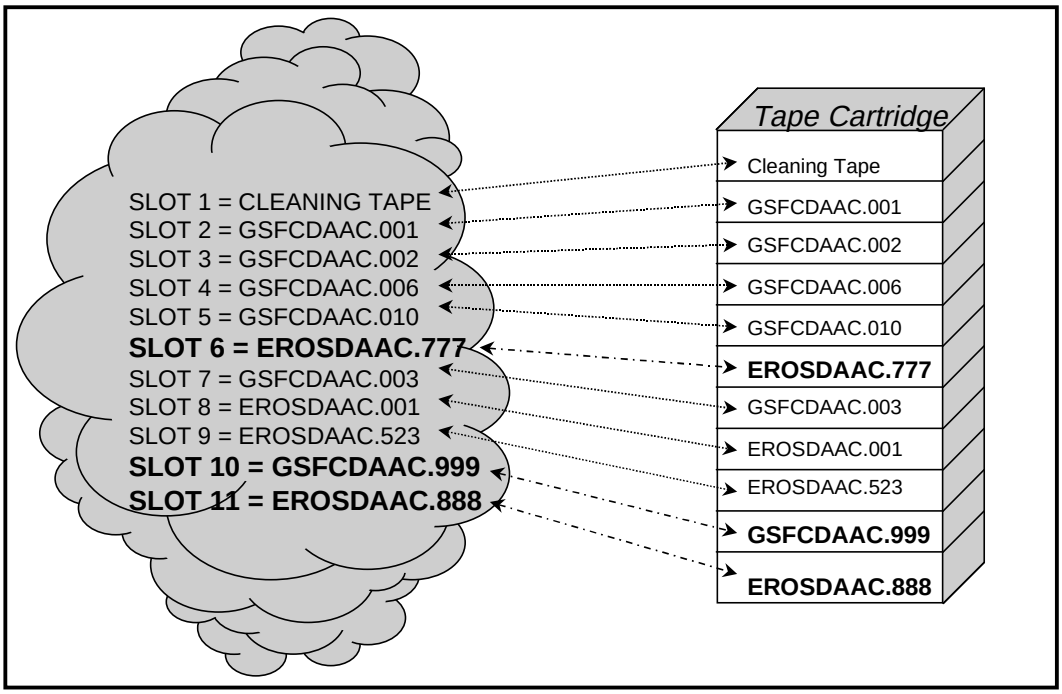

Figure 27. Index is updated after reinventory

Indexing Tape Procedure

---

1 Type **xhost <remote_workstation_name>** and then press the **Enter** key.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**.

3 Start the log-in to the Backup client server by typing **tools/bin/ssh *BackupServerName*** in the second window and then press the **Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return**.

- You are authenticated as root and returned to the UNIX prompt.

8 At the UNIX prompt, type **nwadmin**, then press **Return**.

- A window opens for the **Networker Administrative** program.

9 Click the **Mount** button, or select **Media -> Mount** from the menu.

- The **Jukebox Mounting** window opens (Figure 28) and displays a list of the tapes that Networker is currently aware of.
- When you are finished with this window, click the **Cancel** button.

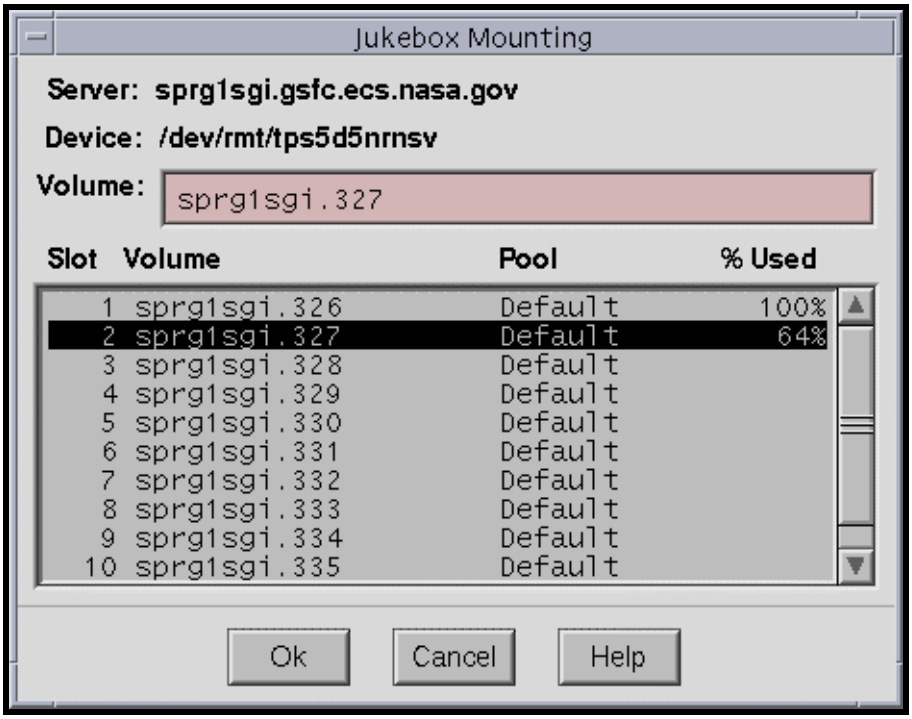

Figure 28. Jukebox Mounting window.

10 Insert the required tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.

- Refer to the jukebox's documentation for detailed instructions on installing the cartridge.

11 Select **Media** from the menu bar, then select **Inventory**.

- The **Jukebox Inventory** window opens.

12 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.

- Slot 1 is at the top of the cartridge and 10 at the bottom.
- Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
- It is OK to leave empty slots or slots with previously inventoried tapes.

13 Click the **OK** button.

- A status message indicating the progress of the tape indexing procedure appears and updates.
- Inventorying a full cartridge of tapes takes between 20 and 30 minutes.

14 When the **Jukebox Inventory** status reads **finished**, click the **Cancel** button.

15 Click the **Mount** button to verify that the indexing worked.

- The **Jukebox Mounting** window opens.
- The **required tape(s)** should be shown. If not, repeat this procedure from step 8.

16 Click the **Cancel** button.

- The **Jukebox Mounting** window closes.

17 From the menu bar, select **File**, then select **Exit**.

18 At the UNIX prompt for the ***BackupServer***, type **exit**, then press **Return**.

19 At the next UNIX prompt, type **exit** again, then press **Return**.

This page intentionally left blank.

System Backups and Restores

Performing regular and comprehensive backups is one of the most important responsibilities a System Administrator has. Backups are the insurance that essentially all of the system data is always available. If the system crashes and all disks are damaged, the System Administrator should be able to restore all of the data from the backup tapes.

Incremental Backup

An incremental backup copies to tape all files on a system or subsystem that were created or modified since the previous incremental backup regardless of the backup level. The purpose of an incremental backup is to insure that the most recent edition of a file is readily available in case user error or disastrous system failure causes the file to become corrupt. Incremental backups are scheduled at a time that causes minimal disruption to the users. Copies of all incremental backup tapes are stored offsite for five weeks before they are reused.

Incremental backups are performed automatically according to the schedule setup in the Networker

Schedules windows (Figure 29). Incremental backups can also be requested at unscheduled times by completing the **Incremental Backup Request Form** and submitting it to the DAAC manager.

On-Demand Incremental Backup Procedure

1 Type **xhost <remote_workstation_name>** and then press the **Enter** key.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**.

3 Start the log-in to the Backup client server by typing **tools/bin/ssh *BackedUpSystemName*** in the second window and then press the **Enter** key.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return.**

7 A password prompt is displayed.

8 Enter the ***RootPassword***, the press **Return**.

- You are authenticated as root and returned to the UNIX prompt.

9 At the UNIX prompt, type **nwadmin**, then press **Return**.

- A window opens for the Networker Administrative program.

10 Go to the **Customize** menu, select **Schedules**.

- The **Schedules** window opens.

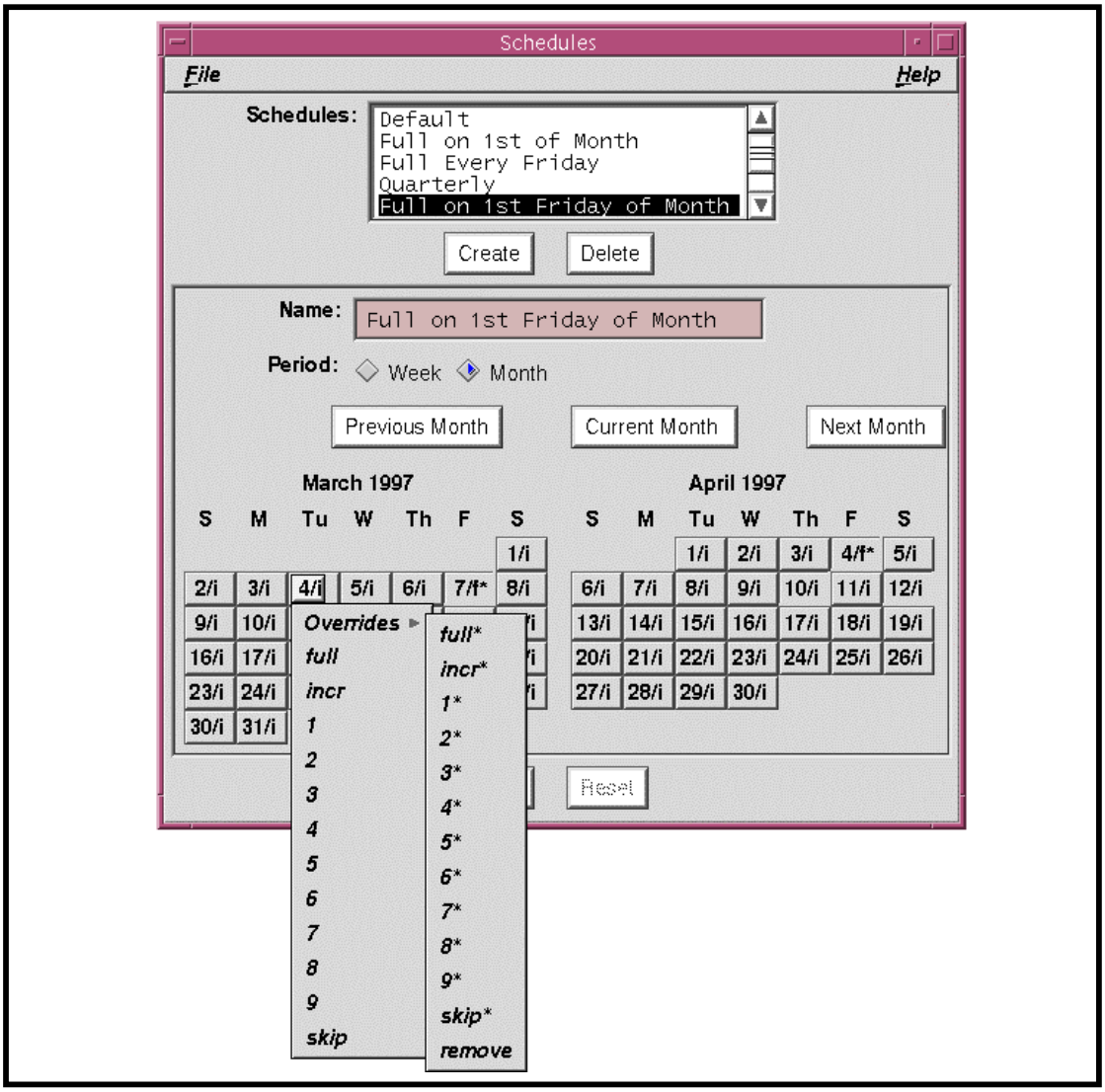

Figure 29. Networker Schedules window

11 Look at the button for today and note the letter on that day. If there is an **i** next to the date on this button, go to step 12.

- The **i** stands for incremental; **f** stands for full. Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.

12 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.

13 Click the **Apply** button.

14 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

15 Click the **Group Control** button.

- The **Group Control** window opens.

16 Click the **Start** button.

- A **Notice** window opens.

17 Click the **OK** button.

- The **Notice** window closes.
- The regularly scheduled backup will still run (even though we are now doing a backup).

18 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.

- Status updates appear in the **nwadmin** window.
- When the backup is complete, a **Finished** message will appear.

19 If the button for today in step 9 had an i on it, go to step 23.

20 Go to the **Customize** menu, select **Schedules**.

- The Schedules window opens.

21 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.

22 Click the **Apply** button.

23 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

24 Select **Exit** from the **File** menu to quit the NetWorker Administrative program.

- The **nwadmin** window closes.

25 At the UNIX prompt for the machine to be backed up, type **exit**, then press **Return**.

- Root is logged out.

26 Type **exit** again, then press **Return**.

- You are logged out and disconnected from the machine to be backed up.

Full System Backup

A full system backup is a snapshot of the data on the entire system as of a particular date. The data is stored on tapes that are used to recreate the system in the event of a total system failure. The full system backup is run by the System Administrator on a regular schedule, usually weekly. Full system backup tapes are stored offsite for security reasons.

Full Backup Procedure

---

1 Type **xhost <remote_workstation_name>** and then press the **Enter** key.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**.

3 Log into the machine to be backed up by typing: **/tools/bin/ssh *BackedUpSystemName***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return**.

- You are authenticated as root and returned to the UNIX prompt.

8 Execute the NetWorker Backup program by entering: **nwbackup**, then press **Return**.

- A **NetWorker Backup** window opens (Figure 30). You are now able to perform a full backup.

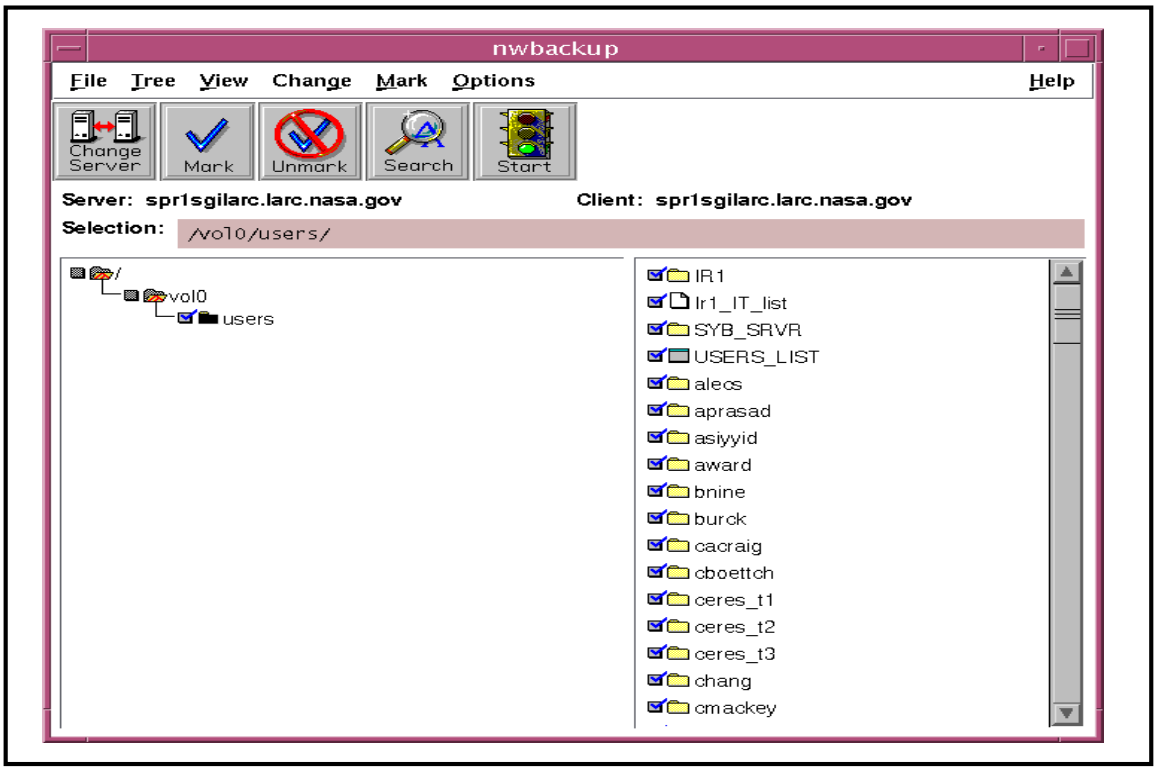

Figure 30. Networker Backup Window

9 If no **files/directories to be backed** up were provided by the requester, i.e. the whole machine is to be backed up, then type **/** in the **Selection** field and click the **Mark** button.

- / is designated for backup and has a check next to it.

10 If **files/directories to be backed up** were provided then select the **files/directories to be backed up** in the directory display and click the **Mark** button.

- Drag scroll bar with mouse to scroll the list up and down.
- Double click on directory name to list its contents.
- To move up a directory level, type the path in the **Selection** field.
- Clicking the **Mark** button designates the file for backup and puts a check next to it.

11 Click the **Start** button.

- A **Backup Options** window opens.

12 Click the **OK** button.

- The **Backup Options** window closes.
- The **Backup Status** window opens providing updates on the backup's progress.

13 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.

- The **Backup Status** window closes.
- The backup is complete.

14 Select **Exit** from the **File** menu to quit the NetWorker Backup program.

- The NetWorker Backup window closes.

15 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.

- Root is logged out.

16 Type **exit** again, then press **Return**.

- You are logged out and disconnected from the machine to be backed up.

Single or Multiple File Restore

From time to time individual files or groups of files (but not all files) will have to be restored from an incremental backup tape due to operator error or system failure.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- Name of machine to be restored.
- Name of file(s) to be restored.
- Date from which to restore.
- User ID of the owner of the file(s) to be restored.
- Choice of action to take when conflicts occur. Choices are:
  - ❑ rename current file.
  - ❑ keep current file.
  - ❑ write over current file with recovered file.

Single or Multiple File Restore Procedure

1 Type **xhost <remote_workstation_name>** and then press the **Enter** key.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**.

3 Log into the machine to be restored by typing: **/tools/bin/ssh *Machine Restored***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return**.

- You are authenticated as root and returned to the UNIX prompt.

8 Log in as the user by typing: **su *User'sID.***

- You are authenticated as the **owner of the file(s) to be restored**.

9 Execute the NetWorker Recovery program by entering: **nwrecover**, then press **Return**.

- A window opens for the **Networker Recovery** program (Figure 31). You are now able to perform restores of files.

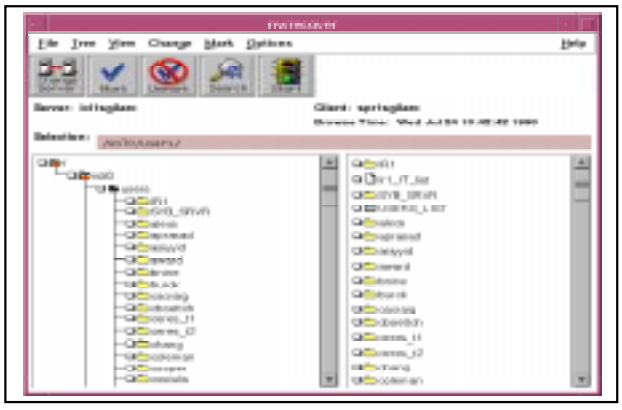

Figure 31. Networker Recovery Window

11 Select **file(s) to be restored** and click the **Mark** button.

- Drag scroll bar with mouse to scroll the list up and down.
- Double click on directory name to list its contents.
- Clicking the **Mark** button designates the file for restore and puts a check next to it.

12 Go to the **Change** menu, select **Browse Time**.

- The **Change Browse Time** window opens.

13 Select the **date from which to restore**.

- Networker will automatically go to that day's or a previous day's backup which contains the file.

14 Click the **Start** button.

- The **Conflict Resolution** window opens.

15 Answer "Do you want to be consulted for conflicts" by clicking the **yes** button, then click the **OK** button.

- If prompted with a conflict, choices of action will be: rename current file, keep current file, or write over current file with recovered file.
- Select the requester's **choice of action to take when conflicts occur.**
- The **Recover Status** window opens providing information about the file restore.
- If all the required tapes are not in the drive, a notice will appear.
- Click the **OK** button in the notice window.
- If prompted for tapes, click cancel in the **Recover Status** window and execute Procedure 3.2.5.1.1 Index Tapes.

16 When a **recovery complete** message appears, click the **Cancel** button.

17 Go to the **File** menu, select **Exit**.

- The Networker Recovery program quits.

18 Type **exit**, then press **Return**.

- The **owner of the file(s) to be restored** is logged out.

19 Type **exit** again, then press **Return**.

- Root is logged out

20 Type **exit** one last time, then press **Return**.

- You are logged out and disconnected from the **machine to be restored**.

Complete System Restore

A complete system restore is an emergency procedure that should be performed only in the event of a system crash with the loss of data and the only way to get the system back up and running in a timely fashion is to restore the system from a previous backup. The result of this action will be that any updates to the system between the last backup and the time of the restore will be lost. The System Administrator will determine which complete backup tape(s) to use (Figure 32). Depending on the frequency of complete system backups and incremental backups, data loss can be minimized.

A complete system restore involves restoring a number of tapes depending upon the particular situation. For example, should a system failure occur immediately after a full system backup was performed, only the tapes used in that backup will be required to restore the system to its usable state. However, if there was a period of time between the last full system backup and the system failure, tapes from the last full system backup as well as partial and incremental backups will have to be restored. This may become a time consuming process depending on the server affected, how much data is to be recovered, and how many tapes need to be restored. Additionally, the System Administrator may determine that only one or two of the many partitions need to be restored to make the system whole again. Therefore, these procedures will have to be mixed and matched to determine the proper restoration procedure for a given situation.

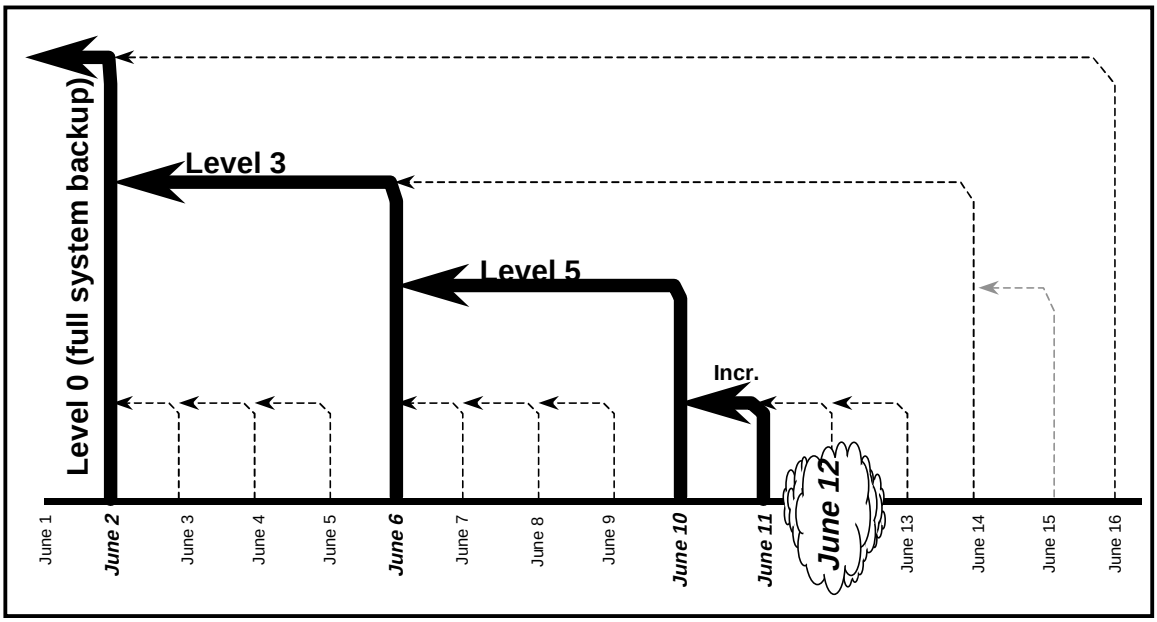

Figure 32. Tapes Required for Full System Restore.

In order to perform the procedure, the SA must have obtained the following information about the requester:

- Name of system to be restored
- Date from which to restore

Full System Restore Procedure

---

1 Log into the backup server by typing: **/tools/bin/ssh *BackupServerName***, then press **Return**.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**.

3 Log into the machine to be restored by typing: **/tools/bin/ssh *Machine Restored***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return**.

- You are authenticated as root and returned to the UNIX prompt.

8 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**.

9 Log in as the user by typing: **su *User'sID*.**

- You are authenticated as the **owner of the file(s) to be restored**.

10 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *MachineRestored*:0.0**, then press **Return**.

11 Execute the Networker Administrator program by entering: **nwadmin**, then press **Return**.

- A window opens for the Networker Administrator program (Figure 33).
- You are now able to perform restores of partitions.

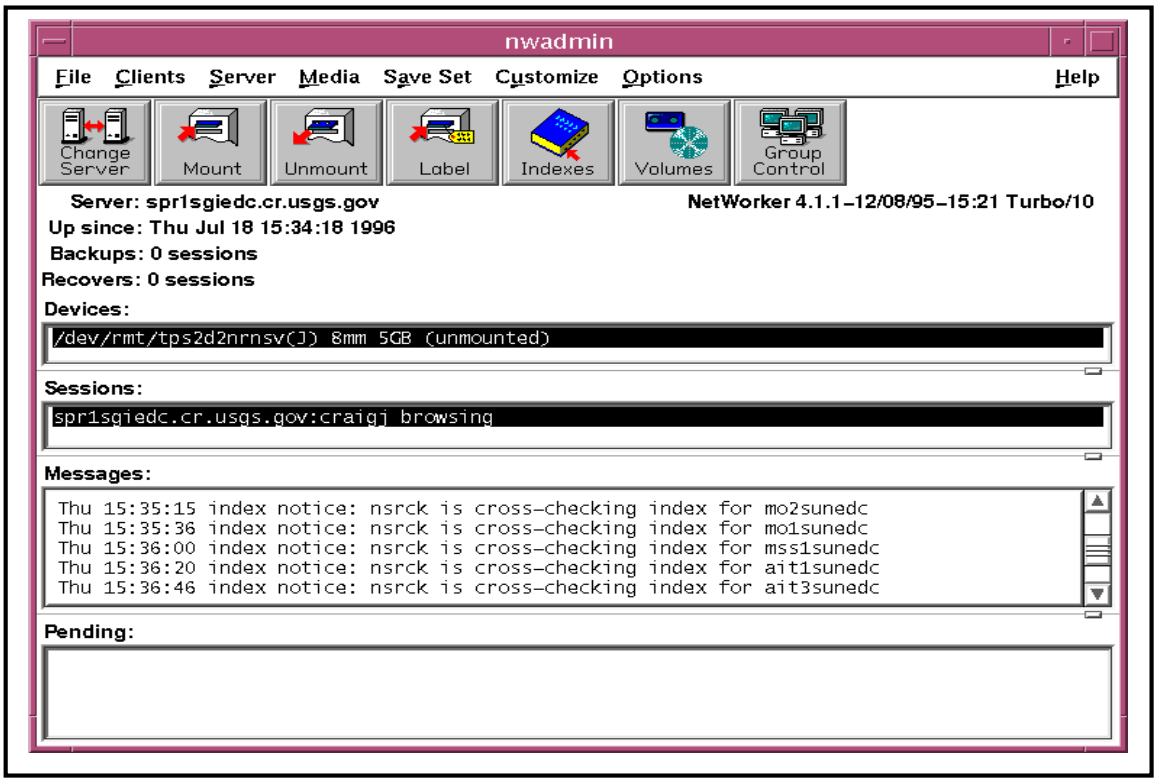

Figure 33. Networker Administrator's Window

12 Go to the **Save Set** menu, select **Recover Set.** The **Save Set Recover** window opens.

13 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.

- The **Save Set** listing updates. This is a listing of partitions on the **System**.
- At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.

14 Select the **Save Set**/partition from the listing.

- The **Instance** listing updates.

15 Select the appropriate **Instance**.

- An **Instance** is a particular NetWorker client backup. A listing of **Instances** is a report detailing the Networker client backups that have occurred.
- Select an **Instance** based upon the **Date from which to restore** (referred to as **Date** in the rest of this procedure) and of an appropriate level:

Note 1: To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backup occurs at 02:00 each morning then a system corrupted at noon on June 6 would require a restoration of the June 6 backup. However, if the system corruption took place around the time of the backup, it would be more prudent to use the backup from June 5.

- If the backups are full or incremental, perform the following actions:

Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.

- If the backups are of different numerical levels, follow these steps:

First select the most recent level 0/full backup prior to or on the **Date** and perform a restore of the partition. If a level 0/full backup did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level 0 and prior to or on the **Date**. Perform a restore of the partition. Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.

- You can double click an **Instance** to see which tape is required.

16 Click the **Recover** button.

- The **Save Set Recover Status** window opens.
- Clicking the **Volumes** button will show which tapes are required.

17 Click the **Options** button.

- The **Save Set Recover Options** window opens.

18 Set Duplicate file resolution to Overwrite existing file by clicking its radio button.

19 Make sure that the **Always prompt** checkbox is not checked.

20 Click the **OK** button.

- The **Save Set Recover Options** window closes.

21 Click the **Start** button in the **Save Set Recover Status** window.

- Status messages appear in the **Status** box.
- A **recovery complete** message appears when recovery is complete.

22 Click the **Cancel** button after the **recovery complete** message appears.

- The **Save Set Recover Status** window closes.

23 If additional partition restores are required, go to step 8. Otherwise, select **Exit** from the **File** menu to quit the Networker Administrator program.

24 At the UNIX prompt for the backup server, type **exit**, then press **Return**.

25 Type **exit** again, then press **Return**.

System Log Maintenance

System Log Maintenance

The System Log Maintenance process is performed through Tivoli by the System Administrator. The System Administrator will setup and execute the jobs to be run in various formats, i.e., recurring day and time, maximum amount of disk space. This section assumes that task jobs have already been created and discusses how to edit the job for System Log Maintenance.

Logs are used to track events on the system. An *event* is the success or failure of an action. By reading and maintaining logs, system administrators can troubleshoot problems. Entries to the logs are automatically created by the particular application and stored in the directory /usr/local/hislog in a file with a *.log* suffix (e.g., IngestLocal.log).

System Log Maintenance Procedure

1 Log in to a **Tivoli server** by typing: **/tools/bin/ssh *TivoliServerName*** at the UNIX prompt, then press **Return**.

2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber*:0.0** or **setenv DISPLAY *BackupServerName*:0.0**, then press **Return**.

3 Log into the machine to be restored by typing: **/tools/bin/ssh *Machine Restored***, then press **Return**.

- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 3.
- If you have not previously set up a secure shell passphrase; go to Step 4.

4 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Enter** key. Go to step 5.

5 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Enter** key.

6 Log in as root by typing **su**, then press **Return.**

- A password prompt is displayed.

7 Enter the ***RootPassword***, the press **Return**.

- You are authenticated as root and returned to the UNIX prompt.

8 Enter **tivoli**, then press **Return**.

- The **TME Desktop Administrator** window (Figure 34) appears.

Figure 34. TME Administrator Window

9 Double-click on the **Scheduler** icon (Figure 35).

Figure 35. Scheduler icon

10 Click once on the job you wish to edit so that it is highlighted.

11 Select **Edit** from the menu at the bottom of the screen.

- You will now be in the **Edit Scheduled Job** window.

12 Make all of the desired changes.

13 After changes have been made, select **Update & Close** from the menu at the bottom of the window.

14 Type **exit**, then press **Return**.

- You are looged out of the Tivoli server.

User Administration

Adding a New User

Adding a user to the system is accomplished through a series of steps that may be performed as a suite from the command line, or by use of a script. The procedure below outlines the individual steps that are required to completely set up a new user on the system. The scripts will accomplish these steps in an interactive manner.

The requester fills out a "User Registration Request Form" and submits it to the supervisor. The requester's supervisor reviews the request, and if s/he determines that it is appropriate for the requester to have an account, forwards the request to the System Administrator. The System Administrator verifies that all required information is contained on the form. If it is, s/he forwards the request to the approval authority; the DAAC Manager. Incomplete forms are returned to the requester's supervisor for additional information. If the request for the accounts fits within policy guidelines, the DAAC Manager approves the request and returns the request form to the System Administrator to implement.

The System Administrator should be familiar with a UNIX text editor and the files **/etc/passwd.yp** (Figure 36), **/etc/group** (Figure 37), and **/etc/auto.home** .

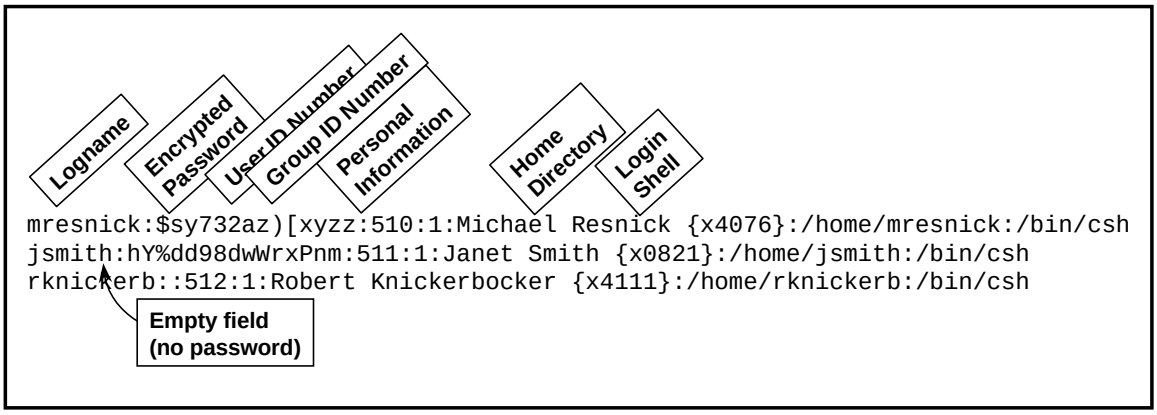

Figure 36. /etc/passwd.yp File Fields

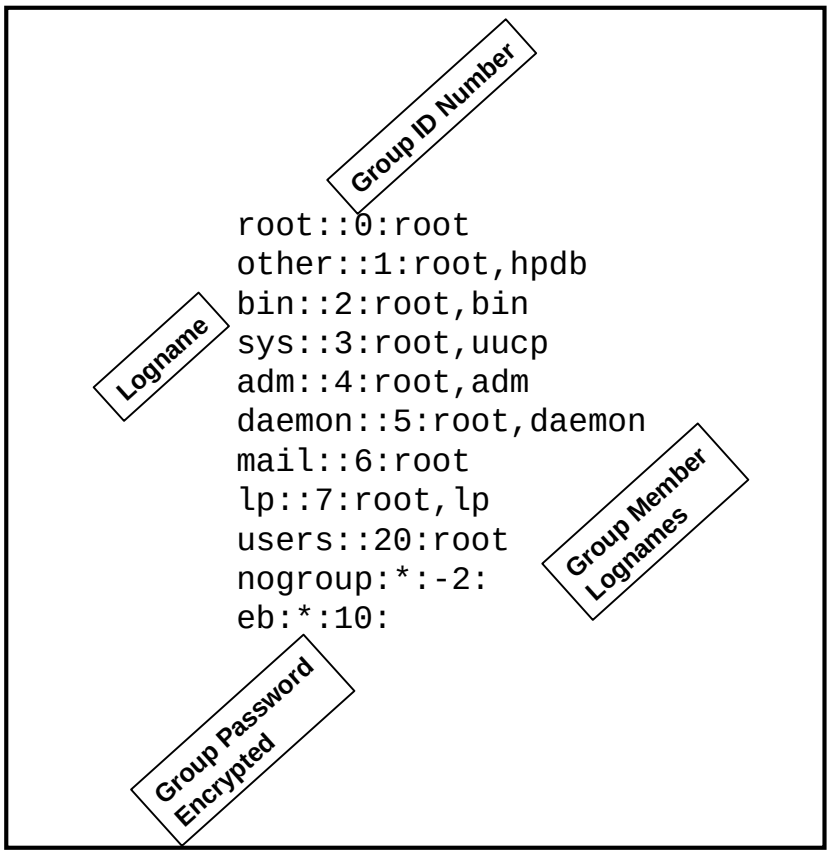

Figure 37. /etc/group File

The SA creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Newuser*, to add new users to the system. The script, which is available to other DAACs, walks the System Administrator through data input of user information, checks for the same user in other systems, creates a User ID, synchronizes password files and creates home directories for new users.

Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for deleting a user has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **UNIX login of the user to be deleted**

b. **Role(s) of the user to be deleted**

The SA deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Lockdown*, to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion, deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

Changing a User's Account Configuration

Account configuration is accomplished through command line and script. The DAAC manager must authorize changes to user account.

The Changing a User Account Configuration process begins when the requester submits a request to the Ops Supervisor detailing what to change about the account configuration and the reason for the change. The Ops Supervisor reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and Ops Supervisor.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- What to change and new settings. Can be any of:
  - ❑ New Real User Name
  - ❑ New Office Number
  - ❑ New Office Phone Number
  - ❑ New Home Phone Number
  - ❑ New UNIX Group
  - ❑ New DCE Group
  - ❑ New DEC Organization
  - ❑ New Login Shell
- Current UNIX Login of the User

Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the Ops Super. The Ops Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and Ops Super.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Role(s) to which the user is to be added
- Role(s) from which the user is to be removed
- UNIX login of the user

Changing a User Password

The Changing a User Password process begins when the requester submits a request to the SA. The SA verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management and that the SA is an administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New password for the user**

To change a user password for the requester, execute the command line or script procedure steps that have been developed.

Checking a File/Directory Access Privilege Status

Checking File/Directory Access Privileges Procedure

1 At a UNIX prompt, type **cd *Path***, press **Return.**

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe, then type **cd /home** and press **Return**.

2 From the UNIX prompt, type **ls -la**. The output from the command should appear as below:

```
drwxrwxrwx    3    mresnick    training    8192    Jun 14 08:34    archive
drwxr-xr-x   11    mresnick    training    4096    Jul 03 12:42    daacdata
-rw-rw-rw-    1    mresnick    training     251    Jan 02 1996     garbage
lrw-r--r--    2    jjones      admin      15237    Apr 30 20:07    junk
-rwxr--rw-    1    mresnick    training    5103    Oct 22 1994     trash
```

- The first column of output is the file access permission level for the file (see Figure 37 below for a description of file permissions).
- The next column to the right is the number of links to other files or directories.
- The third column is the file owner's user ID
- The fourth column is the group membership of that owner.
- The fifth column shows file size in bytes.
- The sixth column displays the date and time of last modification (if the date is more than six months old, the time changes to the year)
- The last column displays the file name.

Changing a File/Directory Access Privilege

File and directory access privileges are displayed in the first output column of the **ls -l** command and consists of ten characters, known as **bits**. Each bit refers to a specific permission. The permissions are divided into four groupings shown and briefly described in Figure 38:

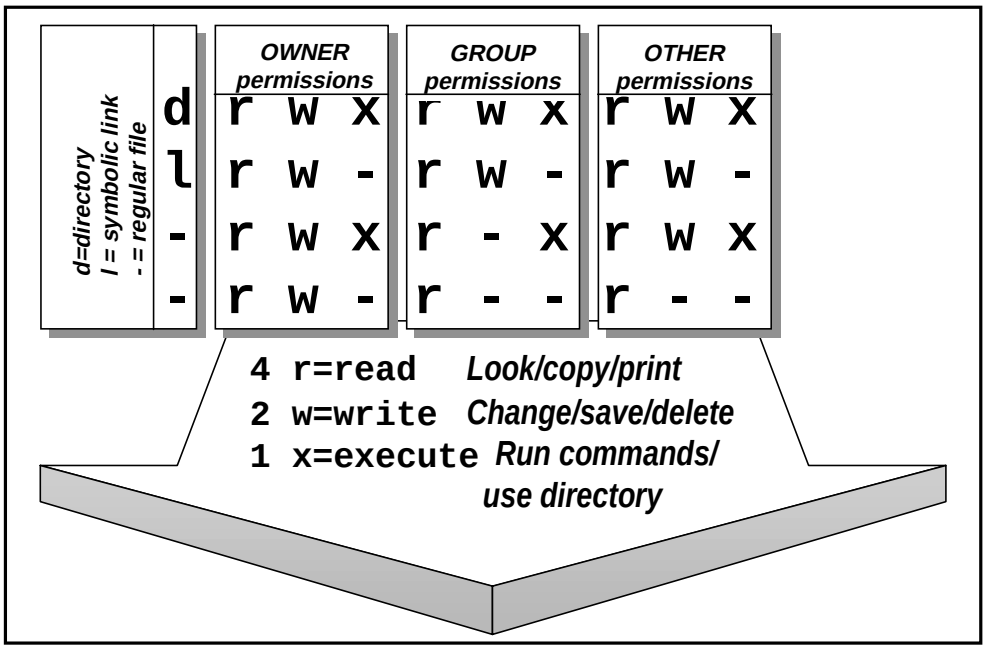

Figure 38. Access permissions

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- full path of the file/directory on which access privileges will be changed.

- new access privileges to set on the file/directory. Can be any of:
  - ❑ New owner
  - ❑ New group
  - ❑ New user/owner privileges (read, write and/or execute)
  - ❑ New group privileges (read, write and/or execute)
  - ❑ New other privileges (read, write and/or execute)

Changing a File/Directory Access Privilege Procedure

---

1 At the UNIX prompt, type **su**, press **Return**.

2 At the **Password** prompt, type ***RootPassword***, press **Return**.

- Remember that ***RootPassword*** is case sensitive.
- You are authenticated as root.

3 Type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe then type **cd /home** and press **Return**.

4 If there is a **New owner** then type **chown *NewOwner FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chown *NewOwner* jdoe** and press **Return**.

5 If there is a **New group** then type **chgrp *NewGroup FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chgrp *NewGroup* jdoe** and press **Return**.

6 If there are **New user/owner privileges** then type **chmod u=*NewUserPrivileges FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod u=*NewUserPrivileges* jdoe**, press **Return**.

- The ***NewUserPrivileges*** are r for read, w for write and x for execute. For example, to give the user/owner read, write and execute privileges, type **chmod u=rwx *FileOrDirectoryName*** and press **Return**.

7 If there are **New group privileges** then type **chmod g=*NewGroupPrivileges* *FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod g=*NewGroupPrivileges* jdoe**, press **Return**.
- The ***NewGroupPrivileges*** are r for read, w for write and x for execute. For example, to give the group read and execute privileges, type **chmod g=rx *FileOrDirectoryName*** and press **Return**.

8 If there are **New other privileges** then type **chmod o=*NewOtherPrivileges* *FileOrDirectoryName***, press **Return**

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type **chmod o=*NewOtherPrivileges* jdoe**, press **Return**.
- The ***NewOtherPrivileges*** are r for read, w for write and x for execute. For example, to give other read privileges, type **chmod o=r *FileOrDirectoryName*** and press **Return**.

9 Type **exit**, press **Return**.

- Root is logged out.

Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the Ops Supervisor. The Ops Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and Ops Supervisor.

This page intentionally left blank.

New Workstation Installation

Installing a new workstation has three stages. Each stage has several sub-tasks that must be performed in a prescribed order. These steps include:

1 Preparation

- Preparing the hardware
- Configuring the network

2 Installation

- Installing the hardware
- Installing the operating system(s)
- Installing the custom software
- Installing the COTS software

3 Testing and Verification

- Rebooting the workstation
- Logging onto the workstation

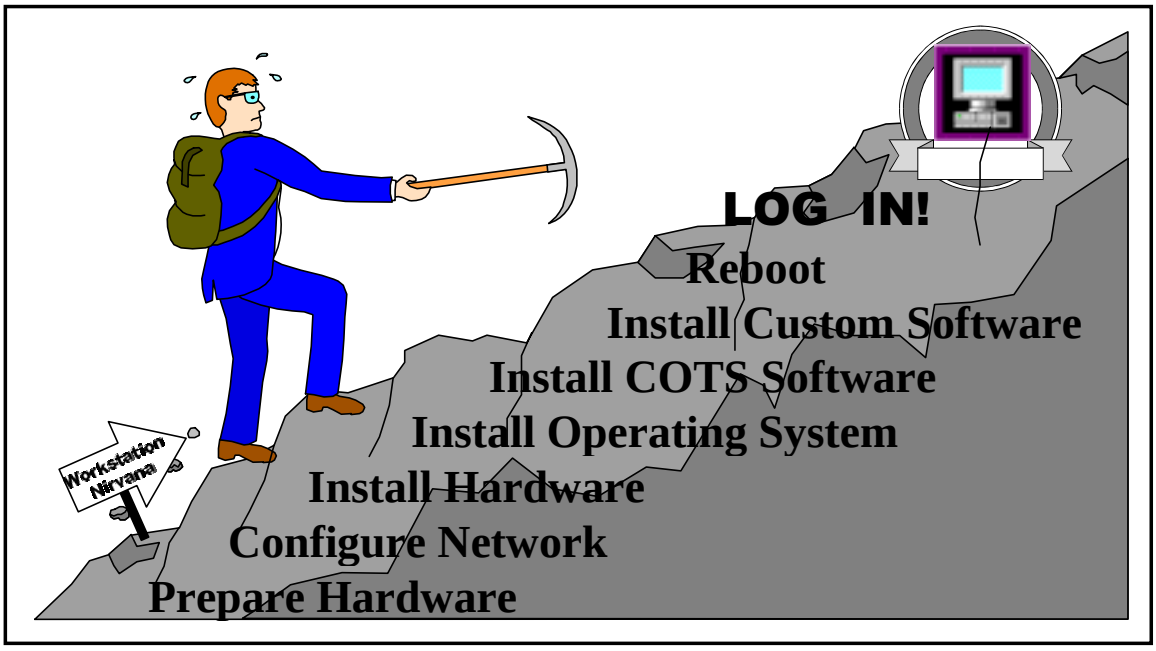

Figure 40. Workstation Installation Steps

Preparation

Hardware Preparation

The Hardware Preparation process begins when the requester submits a request to the System Administrator. The System Administrator then determines if the requested hardware is on hand or must be ordered. Once the hardware is available along with all the necessary attachments, the System Administrator will schedule the installation.

The System Administrator must obtain the following information from the requester:

- type of hardware desired (HP, Sun, SGI or NCD).
- location of installation.

[Refer to Section 3.3 of the Release B Installation Plan (800-TP-0xx-00x) for detailed instruction on how to install hardware.]

Network Configuration

In a nutshell, all network configuration entails is giving the hardware device a name in accordance with the DAAC standard, and forwarding that information to the Network Administrator for assignment of an IP address and its addition to the network domain name service (DNS).

Network Configuration Procedure

1 Determine the name of the hardware.

- For example, if the hardware is a NCD, the name will be **ncd#** where **#** is sequential from the inventory list. If the hardware is a Sun, the name may be personalized (i.e., fred).
- *NOTE*: If the hardware is a NCD, the SA needs to determine the name of the NCD Login Host. The NCD Login Host will be the name of the X-server this NCD will use.

2 Submit a request to the Network Administrator for the IP address and the DNS entry.

Installation

Hardware

The actual installation of the hardware involves the logical steps of:

- removing the hardware from its packaging

- placing the hardware in the location prescribed in the Release A Installation Plan (800-TP-005-001)
- connecting the appropriate cables and wires

When these steps are completed in accordance with the procedures in the Release A Installation Plan (800-TP-005-001), the item(s) must be reported to inventory.

Reporting to Inventory Procedure

1	Locate the Inventory Control Number on each hardware component and record them. The Inventory Control Number is on a small bright sticker on the front of each hardware component.
2	Submit the Inventory Control Numbers and location of the machine to the Inventory Controller.

Operating System Installation

*NOTE: Throughout this section, reference is made to a **download disk**. A download disk is a removable disk drive that is connected to the hardware device onto which software is to be installed.*

Solaris 2.4 Operating System Installation

Solaris 2.4 is also known as Sun OS 2.4. The Solaris 2.4 Operating System Installation process begins when the installation of hardware procedures have been completed.

This section explains how to install the Solaris 2.4 operating system, including network configuration and patch installation. If you would like a listing of the patches installed, please see document number 420-TD-012-001 Release A Sun Solaris Operating System Patch List.

Solaris 2.4 Operating System Installation Procedure

1 Get the download disk.

2 Check that it is set to be target 2.

- The target number is found on the bottom of the disk.
- You can change the target number by hitting the buttons above and below it.

3 Plug the download disk into the Sun

4 Power on the download disk.

- Facing the front of the disk, the power switch is found on the back to the left of the disk.

5 Power on the monitor; power on the Sun.

- When facing the front of the Sun, the power switch is located on the back right.

6 At the > prompt, type **probe-scsi**, then press **Return**.

- Verify that target 2 exists by finding it in the listing that appears. It will appear as **SCSI Disk: scsi(0)disk(2)**.

7 Type **boot disk2 -swr**, then press **Return**.

- The Sun boots up.
- s is for single user; w is for writeable, and r is for reconfigure (required because you added a drive).

8 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk.
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to a UNIX prompt.

9 Type **/download/setup**, press **Return**.

- Status messages will be displayed.

10 When prompted for the Sun's name, type ***SunsName***, press **Return**.

11 When prompted for the Sun's IP address, type ***SunsIP***, press **Return**.

- The Sun's network and hostname are configured.

12 When you are returned to a UNIX prompt, type **/etc/halt**, press **Return**.

13 At the > prompt, power off the download disk.

14 Disconnect the download disk from the Sun.

15 At the > prompt, type **boot -r**, press **Return**.

- The Sun boots up.
- r is for reconfigure (required because you removed a drive).

16 At the **login:** prompt, type **root**, press **Return**.

17 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk. (The Sun uses the download disk's root password until a new one is set.)
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned the UNIX prompt.

18 Type **passwd root**, press **Return**.

19 At the **New password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the Sun.
- Remember that the ***RootPassword*** is case sensitive.

20 At the **Re-enter new password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the Sun.
- This step confirms that the root password has been entered correctly.
- Remember that the ***RootPassword*** is case sensitive.
- The root password for this Sun is set. Inform all authorized personnel of ***RootPassword***.

21 Type **exit**, press **Return**.

- Root is logged out of the SGI.

22 Inform the backup administrator of the new machine.

HP-UX 9.05 Operating System Installation

This section explains how to install the HP-UX 9.05 operating system, including network configuration and patch installation.

HP-UX 9.05 Operating System Installation Procedure

---

1 Get the download disk.

2 Check that it is set to be target 2.

- The target number is found on the back of the disk.
- You can change the target number by hitting the buttons above and below it.

3 Plug the download disk into the HP.

4 Power on the download disk.

- The power switch is located on the back of the drive.

5 Power on the monitor, power on the HP.

- The power switch is located on the right side of the HP, towards the front.
- The HP starts booting up.

6 At the **Selecting a system to boot. To stop selection process press and hold the ESCAPE key** message, press and hold **Escape**.

- You have 10 seconds to press **Escape** before the boot process proceeds.
- The boot process will stop and a menu of boot commands will appear.

7 Select boot scsi.2.0 by typing **b *DeviceSelectionForscsi.2.0* isl**, press **Return**.

- For example, if the Device Selection for scsi.2.0 in the menu is P1 then type **b P1 isl** and then press **Return.**
- **isl** will cause the HP to boot in interactive mode.

8 At the **ISL>** prompt, type **hpux -is boot disk(scsi.2;0)/hp-ux**, press **Return**.

- **-is** causes the HP to boot in single user mode.
- You will be returned to the UNIX prompt.

9 Type **/download/setup**, press **Return**.

- Status messages will be displayed.

10 When prompted for the HP's name, type ***HPsName***, press **Return**.

11 When prompted for the HP's IP address, type ***HPsIP***, press **Return**.

- The HP's network and hostname are configured.

12 When you are returned to a UNIX prompt, type **/etc/shutdown -h -y now**, press **Return**.

- The HP shuts down and comes to a halt.

13 Once the HP has halted, power off the download disk, power off the monitor.

14 Power off the HP.

15 Disconnect the download disk from the HP.

16 Power on the monitor.

17 Power on the HP.

- The HP starts booting up.

18 At the **Selecting a system to boot. To stop selection process press and hold the ESCAPE key** message, press and hold **Escape**.

- You have 10 seconds to press **Escape** before the boot process proceeds.
- The boot process will stop and a menu of boot commands will appear.

19 Select boot scsi.6.0 by typing **b *DeviceSelectionForscsi.6.0***, press **Return**.

- For example, if the Device Selection for scsi.6.0 in the menu is P1 then type **b P1** and press **Return**.

20 At the **login:** prompt, type **root**, press **Return**.

21 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk. (The HP uses the download disk's root password until a new one is set.)
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned the UNIX prompt.

22 Type **passwd root**, press **Return**.

23 At the **New password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the HP.
- Remember that the ***RootPassword*** is case sensitive.

24 At the **Re-enter new password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the HP.
- This step confirms that the root password has been entered correctly.
- Remember that the ***RootPassword*** is case sensitive.
- The root password for this HP is set. Inform all authorized personnel of ***RootPassword***.

25 Type **exit**, press **Return**.

- Root is logged out of the HP.

26 Inform the backup administrator of the new machine.

IRIX 5.3 and 6.2 Operating Systems Installation

This section explains how to install the IRIX 5.3 and 6.2 operating systems, including network configuration and patch installation.

IRIX 5.3 and 6.2 Operating Systems Installation Procedure

---

1 Get the download disk.

2 Check that it is set to be target 2.

- The target number is found on the bottom of the disk.
- You can change the target number by hitting the buttons above and below it.

3 Plug the download disk into the SGI.

4 Power on the download disk.

- The power switch is located on the back of the drive.

5 Power on the monitor; power on the SGI.

- The power switch is located on the front of the SGI, towards the left.

6 At the **Starting up the system**... message, click the **Stop for Maintenance** button.

- You have only a few seconds to click the **Stop for Maintenance** button before the boot process proceeds.
- The boot process will stop and a **System Maintenance** menu will appear.

7 Select **5 Enter Command Monitor**.

- You will be returned to the Command Monitor prompt which is >>.

8 At the >> prompt, type **hinv**, press **Return**.

- Verify that target 2 exists by finding it in the listing that appears. It will appear as **SCSI Disk: scsi(0)disk(2)**.

9 Type **boot -f dksc(0,2,0)sash**, press **Return**.

- The SGI boots from the download disk into the stand alone shell.
- You will be returned to a UNIX prompt.

10 Type **/download/setup**, press **Return**.

- Status messages will be displayed.

11 When prompted for the SGI's name, type ***SGIsName***, press **Return**.

12 When prompted for the SGI's IP address, type ***SGIsIP***, press **Return**.

- The SGI's network and hostname are configured.

13 When you are returned to a UNIX prompt, type **/etc/shutdown -y -g0**, press **Return**.

- The SGI shuts down.
- You will be returned to a >> prompt, a **System Maintenance** menu or a message saying that **this system can be powered off**.

14 Power off the download disk, power off the monitor.

15 Power off the SGI.

16 Disconnect the download disk from the SGI.

17 Power on the monitor.

18 Power on the SGI.

- The SGI starts booting up.

19 At the **login:** prompt, type **root**, press **Return**.

20 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk. (The SGI uses the download disk's root password until a new one is set.)

- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned the UNIX prompt.

21 Type **passwd root**, press **Return**.

22 At the **New password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the SGI.
- Remember that the ***RootPassword*** is case sensitive.

23 At the **Re-enter new password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the SGI.
- This step confirms that the root password has been entered correctly.
- Remember that the ***RootPassword*** is case sensitive.
- The root password for this SGI is set. Inform all authorized personnel of ***RootPassword***.

24 Type **exit**, press **Return**.

- Root is logged out of the SGI.

25 Inform the backup administrator of the new machine.

NCD Operating System Installation

This section explains how to configure the NCD, including putting the necessary start-up files in place on the server.

NCD Operating System Installation Procedure

---

1 Turn on the NCD and monitor. The monitor power button is on the lower front of the monitor. The NCD power switch is on the back, on the right.

- The message **Boot Monitor V*x.x.x*** will appear.

2 Press the **Escape** key twice.

- You have only a few seconds to press the **Escape** key.
- The boot process stops and a boot monitor prompt, >, appears.
- If you do not see a > prompt then press the **Escape** key a few more times.

3 Press the **Setup** key.

- The **Main** menu will appear.

4 Go to the **Keyboard** menu by pressing the **Right Arrow** key.

- The **Keyboard** menu appears.

5 Select **N-101** by pressing the **Down Arrow** key.

- You may need to press the **Down Arrow** key a few times before **N-101** is selected.

6 Go to the **Monitor** menu by pressing the **Right Arrow** key.

- The **Keyboard** menu disappears.
- The **Monitor Resolution** menu appears.

7 Select **1600x1200 65 Hz** by pressing the **Down Arrow** key.

- You may need to press the **Down Arrow** key a few times before **1600x1200 65 Hz** is selected.

8 Press the **Shift** and **T** keys.

- This tests the new monitor resolution setting.

9 Use the **+** and **-** keys on the front of the monitor under the **ADJUST** label to adjust the screen.

10 Press the **STORE** key on the front of the monitor.

- The monitor stores the screen adjustments.

11 Press the **Escape** key.

- The monitor resolution test ends.
- You are returned to the **Main** menu.

12 Go to the **Network** menu by pressing the **Right Arrow** key twice.

- The **Monitor Resolution** menu disappears.
- The **Network** menu appears.

13 Select **NVRAM** for the **Get IP Addresses From** option.

- You can use the **Space Bar** to move between the available options.

14 Press the **Down Arrow** key.

15 Type the ***NCDIPaddress*** for the **Terminal IP Address** option, press the **Down Arrow** key.

- The ***NCDIPaddress*** is in dotted decimal notation, for example, 155.157.21.34.

16 Type the ***StartupFileServerIPaddress*** for the **First Boot Host IP Address** option, press the **Down Arrow** key.

- The ***StartupFileServerIPaddress*** is in dotted decimal notation, for example, 155.157.44.22.
- The ***StartupFileServer*** is the machine where the NCD startup files are stored.

17 Press the **Down Arrow** key twice.

18 Type the ***NCDGatewayIPaddress*** for the **Gateway IP address** option, press the **Down Arrow** key.

- The ***NCDGatewayIPaddress*** is in dotted decimal notation, for example, 155.157.44.22.
- The ***NCDGatewayIPaddress*** is the same as the ***NCDIPaddress*** except the last number/octet is 1. For example, if the ***NCDIPaddress*** is 155.157.21.34, the ***NCDGatewayIPaddress*** is 155.157.21.1.

19 Press the **Down Arrow** key, type the ***BroadcastIPaddress*** for the **Broadcast IP Address** option.

- The ***BroadcastIPaddress*** is in dotted decimal notation, for example, 155.157.44.22.
- The ***BroadcastIPaddress*** is the same as the ***NCDIPaddress*** except the last number/octet is 255. For example, if the ***NCDIPaddress*** is 155.157.21.34, the ***BroadcastIPaddress*** is 155.157.21.255.

20 Press the **Right Arrow** key.

- The **Network** menu disappears.
- The **Boot** menu appears.

21 Type **Xncdhmx_s** for the **Boot File** option, press the **Down Arrow** key.

22 Press the **Down Arrow** key, type **/data/ncd/** for the **NFS Boot Directory** option, press the **Down Arrow** key.

23 Press the **Down Arrow** key, type **/usr/lib/X11/ncd/configs/** for the **UNIX Config Directory** option, press the **Down Arrow** key.

24 Press the **Down Arrow** key, press the **d** key. The **TFTP Order** option is set to **Disabled**.

25 Press the **Down Arrow** key, press the **1** key. The **NFS Order** option is set to **1**.

26 Press the **Down Arrow** key, press the **d** key. The **MOP Order** option is set to **Disabled**.

27 Press the **Down Arrow** key, press the **d** key. The **LOCAL Order** option is set to **Disabled**.

28 Press the **Right Arrow** key.

- The **Boot** menu disappears.
- The **Done** menu appears. **Reboot** is selected.

29 Press the **Return** key.

- The NCD reboots.
- Status messages appear.

30 Log into the ***StartupFileServer*** by typing: **telnet *StartupFileServer*** or **rsh *StartupFileServer*** at a UNIX prompt, then press **Return**.

31 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**. A password prompt is displayed.

32 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

33 Log in as root by typing: **su**, then press **Return**.

- A password prompt is displayed.

34 Enter the ***RootPassword,*** then press **Return**. Remember that the ***RootPassword*** is case sensitive. You are authenticated as root and returned to the UNIX prompt.

35 Type **cd /usr/lib/X11/ncd/configs**, press **Return**.

36 Type **./i**, press **Return**.

- **i** is a script which builds a NCD startup file.

37 Type the last two numbers/octets of the ***NCDIPaddress*** when the script prompts you for the **IP address**, press **Return**. For example, if the ***NCDIPaddress*** is 155.157.21.34 then type **21.34** and then press **Return**.

38 Type the ***NCDLoginHost*** when the script prompts you for the **Login Host**, press **Return**.

- The ***NCDLoginHost*** is the name of one of the X-servers.

39 When the script prompts you for the **NCD Number**, type the ***NCDname*** minus the "ncd" part. For example, if the ***NCDname*** is ncd2 then the **NCD Number** is 2.

- Some status messages appear telling you what the script is doing.
- The script exits.

40 Type **exit**, then press **Return**.

- Root is logged out

41 Type **exit** again, then press **Return**.

- You are logged out and disconnected from the ***StartupFileServer***.

Custom Software

This procedure describes the steps that are executed to perform a software upgrade on an ECS Host. The personnel involved are the Sustaining Engineer, Resource Manager, Production Monitor, and Host Operator.

This procedure assumes that following actions have already been taken:

- The upgrade has been previously scheduled and noted int he resource plan.
- The software upgrade package was obtained by FTP (File Transfer Protocol) and tar tapes including any associated install script/makefile is in ClearCase at the site.
- The detailed steps for installation have been provided in the VDD accompanying the software package.
- The reconfiguration to minimize impact to existing operational resources has been defined.

Custom Software Installation Procedure

1	Resource Manager composes an information message to the affected operators stating that the affected resources will be taken down as scheduled.
2	Resource Manager asks the Production Monitor to verify that the production has completed on the resource as planned.
3	Production Monitor checks current load on target resources and produces a display of the current jobs running on the requested production resources.
4	Production Monitor informs Resource Manager that production jobs are complete.
5	Resource Manager shuts down any processes still running on the impacted host(s).
6	Resource Manager begins shut down procedures to take host off-line.
7	Resource Manager, operators, and Sustaining Engineer receive a message from HP OpenView indicating that the desired host has gone off-line.
8	Resource Manager notifies Sustaining Engineer that the host is available for upgrade.
9	Sustaining Engineer uses the developers' install script stored in Software Change Manager (ClearCase).
10	Sustaining Engineer verifies that all of the paths and directory structures have been created and are correct.
11	Sustaining Engineer runs all of the diagnostic tests to verify that the new upgrade is operating as expected.
12	Sustaining Engineer informs Resource Manager that the upgrade is completed.
13	Resource Manager acknowledges the message from Sustaining Engineer and initiates host start-up commands.
14	Resource Manager, OP, and Sustaining Engineer receive message from HPOV that the host is back on-line.

COTS

The COTS Software Installation process begins after the SA has completed Section 3.5.2.3.1 Custom Software Installation. After the COTS software installation is complete, the SA proceeds to procedure 3.5.3 Testing and Verification.

COTS Software Installation Procedure

1	Refer to the Release A Hardware and Software Mapping Baseline (attached at the end of this document) for your site.
2	For LaRC, refer to document number 420-TD-007-001.

3 For SMC, refer to document number 420-TD-008-001.

4 For GSFC, refer to document number 420-TD-006-001.

5 In the *Release A Hardware and Software Mapping Baseline* for your site, look up which COTS packages need to be installed on the new workstation using the **Subsystem** and hardware type (the **Target Operating System** column in the document) of the new machine.

Testing and Verification

Reboot

Rebooting each system following the installation of the operating system is required so that all operating parameters and variables are properly set. Note that there are two reboot procedures that follow, one for SGI, HP and Sun computers, the other for NCD computers.

Reboot Procedure for SGI, HP and Sun Computers

1 At the UNIX prompt for the workstation, type **su**, press **Return**.

2 At the **Password** prompt, type ***RootPassword***, press **Return**. Remember that ***RootPassword*** is case sensitive. You are authenticated as root.

3 Type **who**, press **Return**. A list of users currently logged into the workstation appears.

4 If users other than root and you are logged in:

- type **wall**,
- press **Return**,
- type **The system is going down in 5 minutes for *Reason*. Please save your work and log off. We apologize for the inconvenience.**,
- press **Return**,
- press **Control-D**,
- wait 5 minutes before proceeding to step 5.

5 Type **/etc/reboot**, then press **Return**. The workstation reboots. Watch the status messages that appear for any errors. If you are returned to a **Login** prompt and saw no errors during the reboot, the reboot was successful. If the reboot was unsuccessful, use the error messages and system logs to figure out what is incorrect in the workstation installation. The system logs are: **/var/adm/messages** for Solaris 2.4/5.4, **/var/adm/SYSLOG** for IRIX 5.3 and 6.2, and /**usr/adm/syslog** and **rc.log** for HP-UX 9.05.

Reboot Procedure for NCD Computers

1	Press the **Setup** key. The **NCD User Services: Console** window will appear.
2	Go to the **Console** menu, select **Reboot**. The **Reboot** window opens asking if it is **OK to reboot the terminal**.
3	Click the **OK** button. The NCD reboots. Watch the status messages that appear.
4	Once the NCD successfully reboots, a login screen appears.
5	If the NCD does not successfully reboot then use the information in the status messages to determine what went wrong in procedure 3.5.2.2.4 NCD Operating System Installation.

Logging In

Now that the hardware and software have been installed, it is time to log onto the workstation to assure that the user authentication system is operating properly.

Logging In Procedure

1 At the **Login** prompt for the workstation, type ***YourUserID***, press **Return**.

2 At the **Password** prompt, type ***YourPassword***, press **Return**.

- Remember that ***YourPassword*** is case sensitive.
- You are logged in and authenticated as yourself.
- You are returned to a UNIX prompt.
- If you are not logged in and returned to a UNIX prompt, logging in was unsuccessful. Follow these steps:

  Execute this procedure one more time.

  If logging in is unsuccessful again, there is a problem with the workstation installation. Continue to step b.

  Type **root** at the **Login** prompt, press **Return**.

  Type ***RootPassword*** at the **Password** prompt, press **Return**.

  Remember that ***RootPassword*** is case sensitive.

  You are authenticated as root and returned to a UNIX prompt.

Check that automount is running by typing **ps -ef | grep auto** or **ps -aux | grep auto**, press **Return**.

If automount is running then you will see output simil that the workstation is operating and is connected to the NIS.

Test Environment Procedure

1	At the UNIX prompt, type **ps -ef	more** or **ps -aux	more**. A screen full of information about the currently running processes is displayed.
2	Look for the processes associated with the custom and COTS software which you installed in the process listing. To move to the next page full of information, press the **Space** bar. If a process is missing in the listing, go back to the installation of that software package to determine what went wrong.
3	Type **cd ~/*YourUserID***, press **Return**.
4	Type **pwd**, press **Return**, use the output to verify that you are in your home directory. This verifies that automount is running and working correctly for the NIS map **auto.home**. You may follow steps similar to steps 3 and 4 for the other NIS maps. This also verifies that the new workstation was able to contact a NIS server

.

This page intentionally left blank.

Contractor Off-the-Shelf (COTS) Administration

What is COTS?

The ECS organization provides maintenance and operations for ECS hardware, software, and firmware systems delivered under the ECS contract at the ECS sites. Commercial off-the-shelf software (SW), firmware, and hardware will be maintained in accordance with the COTS Maintenance Plan, CDRL 613-CD-001-001. The Project maintenance philosophy for software is to provide ECS centralized support for developed items and vendor-directed support for COTS SW.

Installation

ECS Project software consists of COTS, custom, and science software

SW maintenance includes:

- COTS support contract with the SW vendor for license to use, telephone assistance in resolving COTS software problems, obtaining patches and obtaining upgrades.
- Resources, including equipment, software tools and personnel to maintain ECS in accordance with specified functional, performance, and availability requirements.
- Services required to produce, deliver, integrate, install, test, validate and document corrections and modifications of existing ECS software and firmware. The maintenance activity includes: software configuration management (CM) including support for change control, configuration status accounting, audit activities, and software quality assurance (QA). Each site is the CM authority over its own resources subject to ESDIS delegation of roles for ECS management.

Log files

Log files shall be maintained documenting all COTS installations and modifications. These files delineate manufacturer, product, installation date, modification date and all other pertinent configuration data available.

COTS configuration

The COTS software upgrades are subject to CCB approval before they may be loaded on any platform. The ECS SEO notifies the CCB of the upgrade that has been received. The ECS Property Administrator distributes the COTS software upgrade as directed by the CCB. The site Software Maintenance Engineer, Network Administrator, and the System Administrator are

responsible for upgrading the software on the host machine and providing follow-up information to the Configuration Management Administrator (CMA) and the ECS Property Administrator. The site Local Maintenance Coordinator will notify the appropriate personnel (Release Installation Team, System Administrator, Network Administrator, Software Maintenance Engineer) when the COTS software is received and approved by the CCB for installation.

COTS software patches may be provided by the COTS software vendor in response to a DAAC's call requesting assistance in resolving a COTS software problem. The problem may or may not exist at other locations. When a COTS software patch is received directly from a COTS software vendor (this includes downloading the patch from an on-line source), the DAAC's CCB will be informed via CCR prepared by the requesting Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer. It is the responsibility of the Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer to notify the CCB of the patch's receipt, purpose, and installation status and to comply with the CCB decisions. The Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer installs COTS software patches as directed by the CCB.

In addition to providing patches to resolve problems at a particular site, the software vendor will periodically provide changes to COTS software to improve the product; these changes are issued as part of the software maintenance contract. Upgrades are issued to licensees of the basic software package. Therefore, the COTS software upgrades will be shipped to the ECS Property Administrator, who receives and enters them into inventory.

Distributed Computing Environment (DCE)

What is DCE?

Distributed Computing Environment is a large software program that aids in simplifying routine tasks and makes maintaining large computing environments easier for administrators and end users.

DCE provides users with a shared system for running their computer applications regardless of the number, type, size, or location of their computers. When properly configured, users do not need to have a special account on each and every system in order to do their work. They don't have to log into different systems to perform tasks or access files. They don't have to use e-mail to transfer files across systems.

Figure 41 depicts the interrelationship of the various DCE components.

DCE relies on an operating system and the transport services of a network. Threads is built on (or may actually be part of) that operating system, while the Remote Procedure Call (RPC) relies on Threads, an operating system, and a transport service. Built on top of RPC are most of the other DCE services: Distributed Time Service, Cell Directory Service, and Distributed File Service. Security is shown along the side of the diagram because it is a pervasive service that also relies on RPC. Diskless support, relies on some DCE services and adds a few of its own. Applications that use DCE can take advantage of some or all of its services, and are shown at the very top of the picture.

DCE also relies on the notion of clients and servers. Under this notion, servers provide services to clients that request those services. Because of the relative nature of client and server roles in a DCE environment, a single machine may support processes that are both clients and servers, and a single process at times may itself act as both a client and a server.

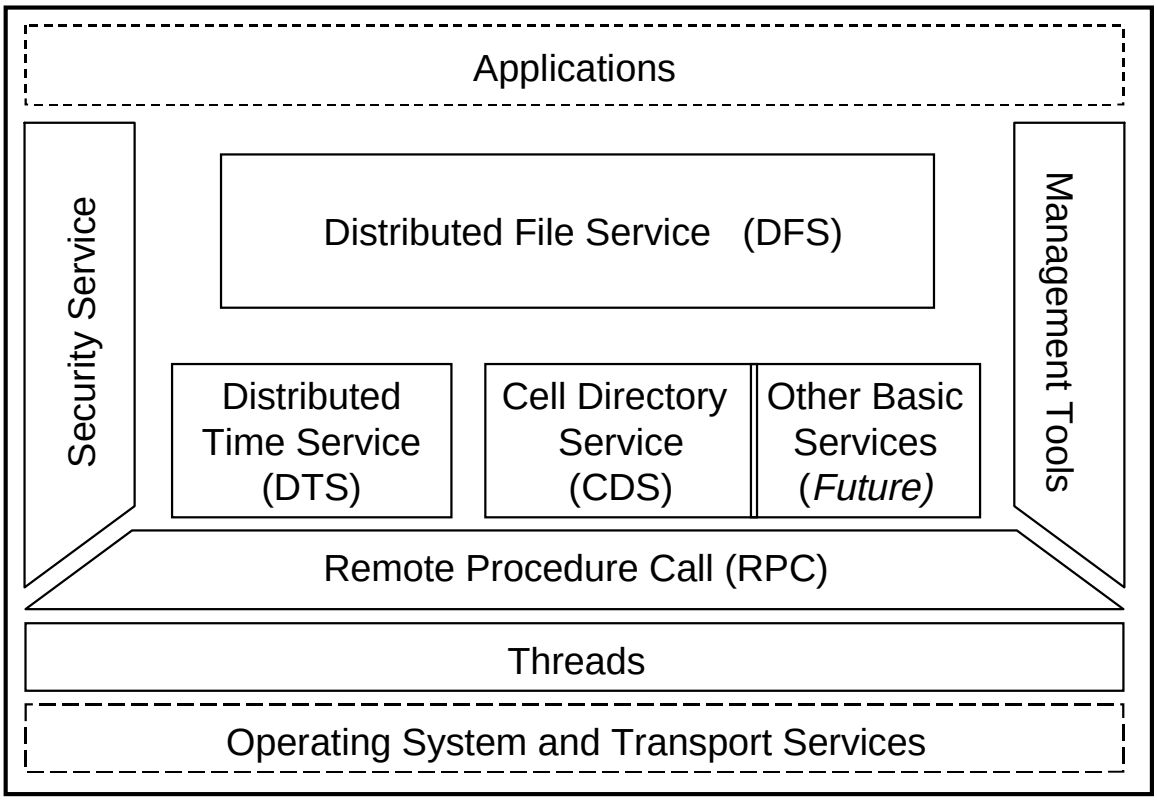

Figure 41. Interrelationship of DCE Components

DCE Terminology

Cell

The cell is the basic unit of operation and administration in DCE. It is a group of systems and resources that typically have a common purpose or share most their communications with each other. A cell usually consists of nodes in a common geographic area (LAN) but may extend beyond the immediate vicinity (WAN). For example, each department in a large organization may be configured as a DCE cell. Consideration must be given to connectivity issues such as speed of transmission (slower over WANs); local administration policies, rules and regulations; and configuration changes.

Each cell is considered to be a single domain for DCE naming and security and all DCE cells are organized into a contiguous namespace, making it easy for clients in one cell to locate and use the services provided in another cell. Each cell must be able to operate independently and thus must supply the essential DCE services, running on one or more server systems, for the DCE clients in the cell.

Each cell must have a Security server and one or more Cell Directory Service servers. Figure 42 shows the topology of a sample DCE cell.

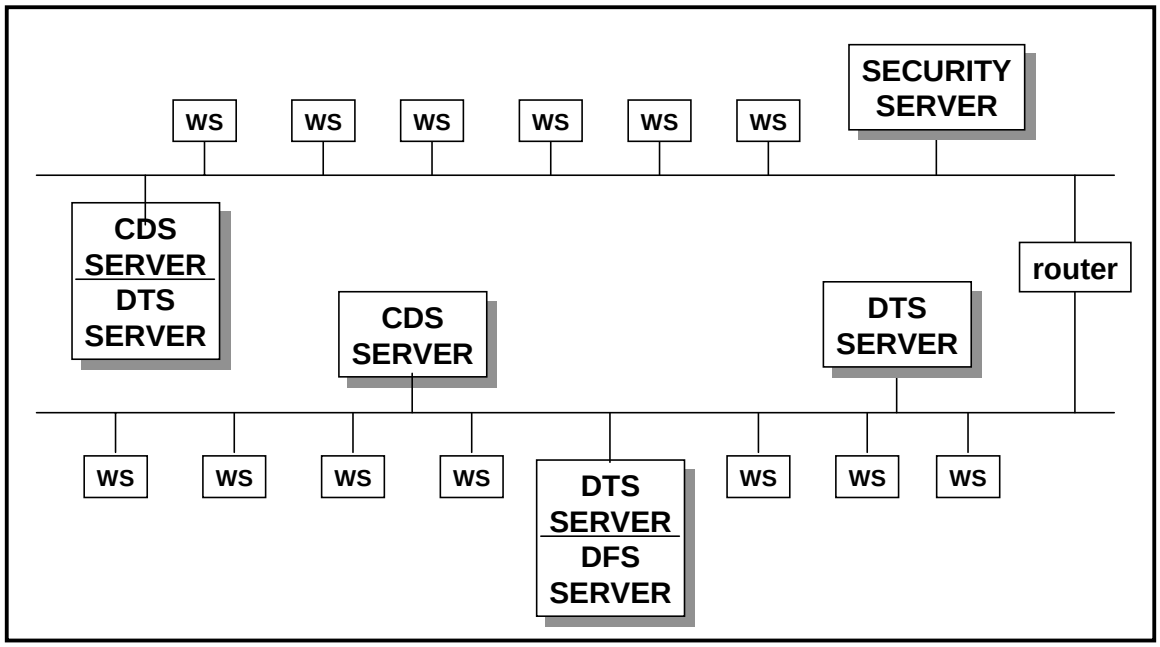

Figure 42. Sample DCE Cell.

Threads

A thread is a single sequential flow of control within a process. It is the active execution of a designated routine, including any nested routine invocations. Within a single thread, there is a single point of execution. With threads, a single process can contain multiple simultaneous flows of execution. Thus, different parts of an application can execute in parallel simultaneously. Although the same thing can be done through multiprocessing, threads do not have the same amount of system overhead as processes and can help to improve application performance.

Remote Procedure Call (RPC)

Remote Procedure Call is a method of implementing communications between the client and the server of an application. Specifically, a remote procedure is one that runs not on the computer from where it is called, but on another computer on the network. RPCs provide a mechanism for distributing processing across a network of computers in a way that masks much of the underlying network complexity.

DCE Directory Service

The DCE Directory Service consists of three components:

- The DCE Cell Directory Service (CDS)

- The DCE Global Directory Service (GDS)
- The DCE Global Directory Agent (GDA)

The **Cell Directory Service (CDS)** stores names and attributes of resources located in a DCE cell. It is optimized for local access since most directory service queries are for information about resources within the same cell as the originator of the query. CDS is replicated, an important feature of a local directory service since the information must be readily available at all times. There must be at least one CDS server in each DCE cell.

The CDS allows objects to be identified by human-readable names and maps those names to the appropriate computer- or network-oriented ID. It also provides location-independence by separating the location of an object from the object itself. Thus, it allows applications and services to easily access an object by using the directory service as a locator.

The **Global Directory Service (GDS)** is a distributed, replicated directory service based on the CCITT X.500/ISO 9594 international standard. It is used when looking up a name outside of the local DCE cell including the worldwide X.500 directory service. Therefore, it acts as a high-level connector and allows independent cells to interact with one another. DCE also supports the use of the Internet Domain Name Service (DNS).

The **Global Directory Agent (GDA)** is the intermediary between a cell's CDS and the rest of the world. It takes a name that cannot be found in the local cell and finds the foreign cell in which the name resides, using GDS or DNS depending on where the foreign cell is registered.

Cell Namespace

The cell namespace is a hierarchical naming convention that is used across the entire distributed environment to provide consistent naming for all distributed objects. DCE supports two kinds of names: global names and local (cell-relative) names. A DCE cell must be named, or registered, in the global namespace to be accessible in the global naming environment. The DCE cell must be named *either* in GDS *or* DNS when it is created, but the cell *cannot* be named in both global namespaces; the cell has exactly one name.

Global names (Figure 43) are universally meaningful and usable from anywhere in the DCE environment. A global name can refer to an object within a cell (CDS) or an object outside the cell (GDS). The prefix **/…** indicates that a name starts at the global root.

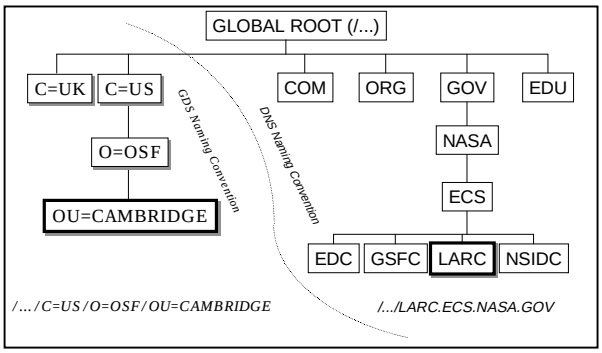

Figure 43. Global namespace naming conventions

Local names (Figure 44) are meaningful and usable only within the cell where that entry exists. As with UNIX file system names, a local, or relative, name is a shortened form of the global name and is a more convenient way to refer to sources within cells. The prefix **/.:** indicates that a name is local, i.e., that it begins at the root of the current cell.

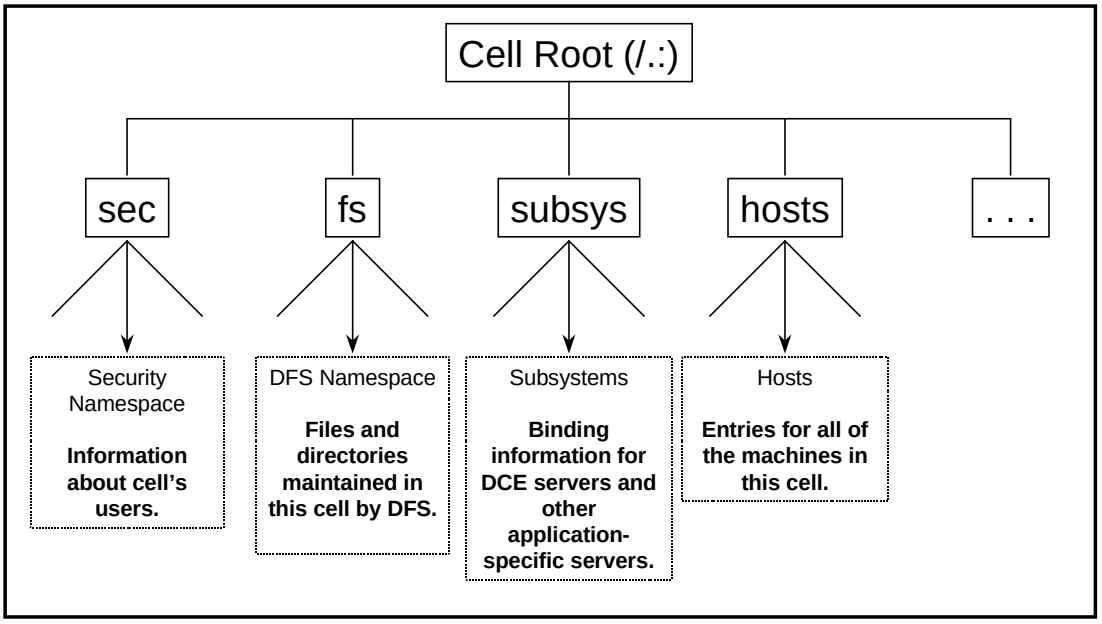

Figure 44. Local namespace naming conventions

GDS Naming Convention is a consistent string of hierarchical elements called Relative Distinguished Names (RDNs). Each name consists of an attribute type and an attribute value separated by an equal sign (=). Each level of attribute is further separated by a slash (/).

DNS Naming Convention uses a different string of hierarchical elements separated by a dot. This is the convention with which most Internet users are familiar and is generally read in reverse order from the lowest portion of the hierarchy to the top (e.g., edc.ecs.nasa.gov).

Distributed Time Service (DTS)

Distributed Time Service synchronizes host clocks on LANs and WANs. This is important because applications require correct and synchronized time for such functions as:

- Event scheduling – applications read the system clock and add a relative time to determine the occurrence of a future event.
- Event sequencing – applications determine the order of events by reading the event report timestamps derived from the system clock.
- Event measurement – applications read the system clock at event start and stop to measure elapsed time.
- Event reporting – applications read the system clock when an event occurs and append a timestamp to the event report or system log.

Clock speeds tend to vary from computer system to computer system. If each system clock in a network started at the same time and ran at the same rate, the clocks would remain synchronized. Because each system clock drifts at a different rate, however, the clocks of systems in a distributed environment tend to become desynchronized. The difference between any two clock readings is called skew. When the accumulated skew reaches a configured threshold, DTS kicks in to update the clocks within the cell. Although all clocks within a cell are synchronized to Coordinated Universal Time (UTC), the actual time on each machine within the cell may still vary. As long as the clocks remain within a range of acceptable values of the UTC time, synchronization is assumed to have been performed.

Synchronization in systems with more than one Time Server functions in a collaborative manner. The Time Clerk queries each of the Time Servers for the correct time, calculates the probable correct time and its inaccuracy based on the answers it receives, and adjusts the local system's time. The adjustment may be made abruptly or it may be an incrementally. For example, if the inaccuracy is only 1 or 2 milliseconds, the change may be made immediately. However, if the skew is larger, say 10 or more milliseconds, then the Clerk increases the clock tick so that the time catches up gradually.

Security Service

The DCE Security Service provides a comprehensive security architecture including authentication, authorization, data integrity, and data privacy.

Initial Cell

The Initial Cell is the first cell that is configured in a DCE environment.

The Configuring the Initial Cell process begins after the Security, CDS, Time and Time Provider servers having been configured, respectively.

NOTE: When planning a DCE cell, note that you must configure a CDS client on any Security server system that is not running a CDS server. You must also configure a Time client on any system that is not running a Time server. Be sure to configure these clients only after you have configured all servers.

Configuring Initial Cell Procedure

---

1 Log in as '**root'** on the machine to be configured as the cell's master Security Server

2 *If it is not already mounted,* mount the Transarc DCE CD-ROM

3 Enter the **dcesetup install** command from the CD-ROM to install the files necessary for DCE client and Security Server configurations

 # /cdrom/dcesetnp install component client secserver \

-dir */cdrom/DCE_version* **[noman] [-mklinks** *network_directorv]*

where

-component client secserver directs the command to install the DCE files necessary to configure the machine as both a DCE client and a Security Server.

-dir */cdrom/DCE_version* specifies the root directory of the DCE files on the CD-ROM. In the pathname, *DCE~version* is the version of DCE being installed (for example, dcel.1).

-noman directs the command not to install DCE reference pages. Omit this option to install DCE reference pages.

4 Enter the **dcesetup config_secserver** command to initiate an interactive Security Server configuration session.

5 Enter the name for your DCE Cell: example: gsfccell.gsfcb.ecs.nasa.gov. The name you specify is used as the name for the cell. DNS-style naming is preferable, to enable cross-cell authentication.

```
Cell name: (<string>, q, ?)
Enter the name of your DCE cell (for example,
gsfccell.gsfcb.ecs.nasa.gov).
```

6 Enter the name of the Cell Administration account or you can use the preferred default name (cell_admin).

```
Cell Administrator's account name: (<string>, q, ?)
[cell_admin]
```

7 Enter the cell_adminstrator's password:

8 **Re**-type the cell_adminstrator's password

9 The following prompt asks whether the machine is to be configured as the master Security Server for your DCE cell:

Is this machine to be cell's "master Security Server"? (y, n, q, ?) [n]

Enter y to indicate that the machine is to be configured as your cell's master Security Server.

10 The following prompt asks for the lowest UNIX user identification number (UID) that the DCE Security Service can generate for principals added to the registry database:

LOW Principal UNIX ID: (<number>, g, ?) [100]

Press <Return> to use the default lowest UID, 100, or enter a different number. Specify **a minimum UID that is** greater than the highest **UID** in your current /**etc/passwd** file; **this minimizes** potential conflicts when you import existing UlDs from your current **/etc/passwd** file into the registry database. Note that this limit applies only to UlDs automatically generated by the DCE Security Service; you can explicitly assign a UID lower than this number to any principal that you create.

11 The following prompt asks for the lowest UNIX group identification number (GID) that the DCE Security Service can generate for groups added to the registry database:

Low Group UNIX ID: (<number>, q, ?) [100]

Press **<Return>** to use the default lowest GID, **100, or enter a different number.** Specify **a minimum GID** that is greater than the highest **GID** in your current /etc/group file; this minimizes potential conflicts when you import existing GIDs from your current /etc/group file into the registry database. Note that this limit applies only to GIDs automatically generated by the DCE Security Service; you can explicitly assign a GID lower than this number to any group that you create.

12 The following prompt asks you to specify the UID for the cell administrator you named in Step *6:*

cell_administrator's UNIX ID: `(<number>, q, ?) [100]`

where *cell_administrator* is the name of the cell administrator's account you specified in Step 6. Press **<Return>** to use the default LID for the cell administrator, **100, or** enter a different UID. Specify a UID that is greater than the highest UID in your current /etc/passwd file.

This system is now configured as the Master Security server. You must now create a CDS server, either on this system or on another system.

After you configure the master Security Server for your cell, your must configure your cell's first CDS Server. A CDS Server stores a clearinghouse, which contains the master or read-only replicas of one or more directories in the cell's CDS namespace. Configuring the first CDS Server creates the cell's namespace.

Configuring DTS Servers

Unlike CDS servers, which can store different sets of information and be positioned within the network to provide convenient access for a particular group of users, the Distributed Time Service servers exist to provide only one thing to the entire cell: synchronized time. After the CDS server has been configured the Distributed Time Service (DTS) server can be configured.

If the DTS server is not already on a system that is configured as a Security or Directory server, repeat steps 1-4 of the Configuring the Initial Cell procedure on that system, and then continue with the steps below. If the DTS server is on a system already configured as a Security or Directory server, continue with step 1 below.

Configuring DTS Servers Procedure

1 If the machine to be configured as a DTS Server is not already configured as a DCE client, configure it as a DCE client according to the instructions.

2 Log in as root on the machine to be configured as a DTS Server.

3 Enter the dcesetup config_dtsserver command to initiate an interactive DTS Server configuration session. The dcesetup command prompts you for the information necessary to configure the machine as a DTS Server.

```
# /etc/dcesetup config_dtsserver
```

4 The following prompt requests the name of the cell administrator's account for your cell:

Cell Administrator's account name: (<string>, q, ?) [cell~admin]

Enter the name you assigned to the cell administrator's account when you configured the master Security Server for your cell. Press <Return> if you used the default account name, cell_admin as the cell administrator's account for your cell.

5 The following prompt asks for the password for your cell administrator's account:

cell_administrator's password:

where *cell_administrator* is the name of the cell administrator's account you specified in the previous step. Enter the password for the specified account.

6 The following prompt asks whether the machine is to be configured as a DTS Local Server or a DTS Global Server:

Type of DTS server configuration (local or global):

(<string, q, ?) [local]

Press <Return> to configure the machine as a DTS Local Server; enter **global to configure** the machine as a DTS Global Server.

7 The following prompt asks if any further DTS configuration is to be made to the machine:

Further DTS server configuration for this machine

(none, courier, backupcourier, or timeprovider):

(<string, q, ?) [none]

Enter one of the following responses.

<Return> specifies that no lurther DTS configuration is to be made to the machine. The machine is configured only as a DTS Local or Global Server, depending on your response to the previous prompt.

courier configures the machine as a courier. A courier periodically synchronizes the machine's clock with clocks on machines configured as DTS Global Servers in its cell.

backupcourier configures the machine as a backup courier. A backup courier assumes the role of courier if no other courier is available in its LAN.

timeprovider specifies that the machine is to be connected to a Time Provider. Connect the machine to a Time Provider to allow it to obtain the current time from a source known to be synchronized with Coordinated Universal Time UTC). If you choose this response, the command prompts for the Time Provider to which the machine is to be connected.

If you choose response none, courier, or **backupcourier,** no further prompts are displayed.

8 *If you entered* **timeprovider** *at the previous prompt,* the following prompt asks for the Time Provider to which the machine is to be connected:

Type of Time Provider to use (null or ntp):

(<string>, q, ?) [null]

Enter one of the following responses:

<Return> specifies that the machine is to use its own clock as a source of current time. Choose this response only if the machine already obtains the current time from an external source. If you choose this response, the DTS Server on the machine does not set the machine's clock, but other DTS clerks and servers can obtain the current time from the machine. if you choose this response, no further prompts are displayed.

ntp specifies that the machine is to obtain the current time from a machine configured **as an** NTP Server. Choose this response only if no other time synchronization mechanism (such as an NTP daemon) is running on the machine. If you choose this response, the command prompts for the name of the NTP Server machine from which the machine is to obtain the current time.

9 *If you entered* **ntp** *at the previous prompt,* the following prompt asks for the name of the **NTP** Server machine from which the machine is to obtain the current time:

NT Provider hostname: (<string>, q, 7)

Enter the name of an NTP Server machine. Specify the name in internet dotted notation (for example, purple.sbc.com).

- The machine is now configured as a DTS Local or Global Server.

Additional CDS Servers

The Configuring Additional CDS Servers process begins after the DTS servers have been configured. This section explains how to configure additional CDS servers.

Configure Additional CDS Servers Procedure

1 If the machine to be configured as an additional CDS Server is not already configured as a DCE client, configure it as a DCE client.

2 Log in as **root** on the machine to be configured as an additional CDS Server.

3 *If it is not already mounted,* mount the Transarc DCE CD-ROM according to the instructions.

4 Enter the dcesetup install command to install the files necessary for a CDS Server configuration:

/etc/dcesetup install -component cdsserver -dir /cdrom/DCE_version \
[-mkiinks *network_director*]

where

-component cdsserver directs the command to install the DCE files necessary to configure the machine as a CDS Server.
-dir */cdrom/DCE_version* specifies the root directory of the DCE files on the CD-ROM. In the pathname *DCE_version* is the version of the DCE files being installed.
-mklinks *network_directory* directs the command to perform a linked installation to the files in a network directory. If the machine uses a linked installation, use this option to name the network directory to which links are created from the machine; if the machine uses a local installation, omit this option.

5 Enter the dcesetup config_cdsserver command to initiate an interactive CDS Server configuration session. The dcesetup command prompts you for the information necessary to configure the machine as an additional CDS Server:

/etc/dcesetup config_cdsserver

Note: Because the machine is already configured as a DCE client, the command displays the following message (in the message, *cell_name* is the name of your DCE cell):

Using the cell_name from previous configuration: *cell_name* If this cell_name is not correct, quit this configuration session, unconf igure, and then reconfigure.

6 The following prompt requests the name of the cell administrator's account for your cell:

Cell Administrator's account name: (<string>, q, ?) [cell_admin]

Enter the name you assigned to the cell administrator's account when you configured the master Security Server for your cell. Press <Return> if you used the default account name, cell_admin, as the cell administrator's account for your cell.

7 The following prompt asks for the password for your cell administrator's account:

cell_administrator's password:

where *cell_administrator* is the name of the cell administrator's account you specified in the previous step. Enter the password for the specified account.

8 The following prompt asks whether the machine is to be configured as the first CDS Server for your DCE cell:

Is this the first CDS Server to be configured in this cell? (y, n, q, ?) [n]

Press <Return> to indicate that the machine is to be configured as an additional CDS Server.

9 The following prompt asks for a CDS name for the clearinghouse to be created on the CDS Server:

Local clearinghouse name: (<string>, q, ?) *[hostname*_ch*]*

Specify the last component of the name by which the CDS clearinghouse on this CDS Server is to be identified in the CDS namespace. The default CDS name for a clearinghouse is *hostname*_ch, where *hostname* is the first component of the name of the machine; for example, if the machine is named blue.abc.com, the default name for the clearinghouse is blue_ch (the corresponding entry in CDS is /.:/blue_ch).

Note: Only the root of the CDS namespace is replicated in the new clearinghouse by default. See the *Transarc DCE Administration Guide* for information about replicating other directories in the clearinghouse.

The machine is now configured as an additional CDS Server.

Notes on Configuring Additional CDS Servers

Immediately after configuring an additional CDS server, you should skulk the root directory using the set directory /.: to skulk command as cell_admin in cdscp. This will initiate the propagation of a consistent copy of the changed root directory information to all the CDS servers, and will prevent problems which might arise from use of inconsistent information before this propagation. The use of several CDS servers may increase the time required to complete the propagation of this information.

Configuration of additional CDS servers can occasionally fail if namespace information is not correctly propagated. Typical failures observe from this cause are:

ERROR: Error during creation of clearinghouse /.:/nodename_ch.

Message from cdscp:

Failure in routine: cp_create_clh; code = 282109010

Requested operation would result in lost connectivity to root directory (dce / cds)

ERROR: Error during creation of clearinghouse / .:/nodename_ch.

Message from cdscp:

Failure in routine: cp_create_clh; code = 282108908

Unable to communicate with any CDS server (dce / cds)

If this happens, the server daemon cdsd has been successfully launched, but its clearinghouse has not been properly created. The clearinghouse is in an intermediate state and cannot be used or deleted, although the rest of the cell namespace and other servers are unaffected. To recover, skulk the root directory, and then use the create clearinghouse /.:/nodename_ch command as cell_admin in cdscp on the new CDS server node to manually complete the configuration of the new server and its clearinghouse. Then skulk the root directory again.

In rare circumstances, you may see the following error when configuring a CDS client or additional server:

ERROR: cdscp error during "define cached server" command.

Message from cdscp:

Failure in routine: cp_define_cached_server; code = 282111142

Cached Server clearinghouse already exists (dce / cds)

This error is benign; and results from the system trying to repeat an operation that has already been done. This error may be ignored.

Security and CDS Client Systems

Before configuring clients, configure server systems as described in the Initial Cell Configuration, Configuring DTS Servers, and Configuring Additional CDS Servers sections. Then use this procedure to configure client systems.

This section explains how to configure security and CDS client systems. To begin configuring the security and CDS client systems, execute the procedures steps that follow:

You must configure a CDS client on any Security server system that is not running a CDS server. To configure a client system, you need to know the name of the Security server and the initial CDS server for the cell.

Note that this procedure does not create a DTS clerk (client). This is described in section 3.6.5.

DTS Clerks

You must configure a DTS clerk (client) on any system not running a DTS server. A DTS clerk is not stared automatically via the dce_config "DCE Client" menu option; you must explicitly start a DTS clerk from the "DTS" menu under "Additional Server Configuration".

Configuring DTS Clerks Procedure

1 Start **dce_config** on the system that you wish to configure with a DTS clerk.

2 You must be logged in as **root** to perform this step.

3 From the **DCE Main** menu, select **Configure** (selection 1).

4 From the **DCE Configuration** menu, select **Additional Server Configuration** (selection 2).

5 From the **Additional Server Configuration** menu, select **DTS** (selection 2).

6 From the **DTS Configuration** menu, select **DTS Clerk** (selection 3).

- This node is now a DTS clerk.

CDS Servers

The DCE Global Directory Agent (GDA) facilitates communication between DCE cells. This section describes how to start the GDA server. A GDA server can only be configured on an exiting client system or CDS server system.

Configuring GDA Servers Procedure

1 From the DCE Main menu, select "Configure" (selection 1).

2 From the DCE Configuration menu, select "Additional Server Configuration" (selection 2).

3 From the Additional Server Configuration menu, select "GDA Server" (selection 7).

- The system configures the GDA server and starts the GDA server daemon, gdad.

Creating a Security Server Replica

A new feature of HP DCE/9000 is Security Server Replication, which provides for improved cell performance and reliability. These steps will allow you to create a security replica via dce_config.

Creating a Security Server Replica Procedure

1 From the **DCE Main** menu, select **Configure** (selection 1).

2 From the **DCE Configuration** menu, select **Additional Server Configuration** (selection 2).

3 From the **Additional Server Configuration** menu, select **Replica Security Server** (selection 8).

4 Enter the **keyseed** for the initial database master key.

- The default name for the replica is **subsys/dce/sec/$HOSTNAME**. If you wish to change the name of the security replica that is created by dce_config, change the value of SEC_REPLICA, either in the file /opt/dcelocal/etcdce_com_env or in the shell environment from which dce_config is run. Note that you must do this before running dce_config

Unconfiguring DCE Client

The **UNCONFIGURE** option removes the target machine from the cell Security database and the CDS namespace. DCE daemons must be running on the system executing the **UNCONFIGURE** option If daemons have been stopped, use the **START** option on the DCE

Main Menu to restart them before using **UNCONFIGURE**. A successfully configured client system can be unconfigured locally. If there were any errors in configuring the client system as a security or directory service client, then the client must be unconfigured from some other system in the cell. Do not use the **UNCONFIGURE** option on a system that is used as a Security server or a CDS server. The **UNCONFIGURE** option removes the system from a cell. If the system is used as a Security server or a CDS server, **UNCONFIGURE** will break the cell.

Unconfiguring DCE Client Procedure

1 Log in as **root** on the machine from which DCE configuration files are to be removed.

2 Enter the **dcesetup unconfig** command to remove DCE configuration files:

/**etc/dcesetup unconfig**

3 The following prompt requests the name of the cell administrator's account for your cell:

Cell Administrator's account name: (<string>, q, ?)

[cell_admin]

4 Enter the name you assigned to the cell administrator's account when you configured the master Security Server for your cell. Press **<Return>** if you used the default account name, **cell_admin**, as the cell administrator's account for your cell.

5 The following prompt asks for the password for the cell administrator's specified with the **-cell_admin** option:

cell_administrator's password

where *cell_administrator* is the name of the specified cell administrator's account. Enter the password for the specified account.

Note: Depending on the configuration of the machine from which files are being removed, you can receive a message reporting a user identification failure. You can safely ignore the message; in most cases, the command succeeds nonetheless.

6 The following prompt asks whether to perform unconfiguration:

Force unconfiguration? (y, n, q, ?) [n]

Press <**Return>** if you do not want a forced unconfiguration. If you no not use a forced unconfiguration, the command will prompt for confirmation before it removes an exisiting database. Enter **y** if you do want a forced unconfiguration.

A forced unconfiguration directs the command *not* to prompt before it removes files for the registry database, a CDS clearinghouse, the FLDB, or the Backup Database. A forced unconfiguration also directs the command to ignore certain error conditions that can arise when removing configuration files.

If authentication fails, local configuration files will be removed but the machine will not be unconfigured in remote databases.

Note: *Use the forced unconfiguration with care*. By default, the command does not remove master replicas of CDS directories. Using a forced unconfiguration directs the command to remove a CDS clearinghouse that houses master replicas of directories and all read-only replicas of those directories in other clearinghouses. Using the option on the CDS Server that stores the master replica of /.: for your cell causes the command to remove your entire CDS namespace.

Note that you must use forced unconfiguration to remove a clearinghouse that contains one or more master replicas. If you enter **n**, the command will display messages like the following:

Unable to delete clearinghouse /.:/clearinghouse. Make sure that this clearinghouse does not house a master replica of any directory or use the -force switch.

7 *If you are removing configuration files from a machine configured as a DFS client or some type of DFS server*, the command displays the following message:

Please gracefully shutdown and restart your system now to stop the kernel -space DFS daemons. After you system comes back up, please reissue the "dcesetup unconfig -force" command to remove remaining configuration data.

dcesetup failed. Details may be available in the /opt/dcelocal/var/adm/messages/dcesetup/log log file.

If you receive this message, reboot the machine a repeat steps 1 through 5; you must include the **-force** option when you issue the **dcesetup unconfig** command the second time. If you do not receive this message, removal of the configuration files is complete.

Note: If you are unconfiguring a DFS File Server that has failed entries in the FLDB, the **dcesetup unconfig** command will fail, even if you are using the **-force** option. The **dcesetup unconfig** command can only unconfigure a DFS File Server that has no fileset entries in the FLDB. See the *Transarc DCE DFS Administration Guide* and the *DCE DFS Admininstration Reference* for information about removing fileset entries from FLDB.

All DCE processes on the machine are now stopped and all DCE configuration files are removed from the machine.

This page intentionally left blank.

Security

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. The Open Software Foundation's Distributed Computing Environment (OSF/DCE) is the primary tool for providing user authentication and authorization, access control, and data integrity. DCE Cell Manager is the administrative tool used to manage a group of users, their access privileges, and system architecture. DCE employs Kerberos and Access Control Lists (ACL) for authenticating users. To monitor and control access to network services, ECS Security Services uses the public domain tool, TCP Wrappers. Three other public domain COTS products — npassword, Crack, and SATAN — provide additional password protection for local system and network access. The tool, Tripwire, monitors changes to files and flags any unauthorized changes.

This section defines step-by-step procedures for M&O personnel to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management.

Running Security Management Log Analysis Program

To log in to the DCE cell Manager, you should login as system **root** before starting DCE cell Manager.

Running Security Management Log Analysis Program

1 Type **/opt/cellmgr/bin/cellManager.**

2 In the Login Name text field, enter ***YourUserID*** then press **Return.**

3 Enter ***YourPassword*** then press **Return.**

4 Click the **LogIn** button if you are logging in with a name and password.

- DCE recognizes you as an authenticated user and the DCE Cell Manager Launcher appears, ***or***
- Click the **LogIn No Security** button if you are logging in as an unauthenticated user.

5 The DCE Cell Manager Launcher appears and provides the following options:

- Namespace Manager - provides a directory tree structure.
- Configuration Manager - identifies hosts currently configured in the cell.

- Security Manager - shows the organizations in the registry and represents the organization domain.
- Preferences - brings up DCE Launcher preferences.
- Help - provides information on interface.
- Exit - provides options for exiting.

6 Click one of the option buttons one time to start a DCE Cell Manager tool, to start an application you previously added to the Launcher, or to add another button to the Launcher window (Preferences button). The selected button becomes temporarily insensitive while the tool starts its initialization routines. (Clicking more than once will launch multiple copies of the same tool.) You can have more than one tool active at the same time.

Generating Security Reports

Reviewing User Activity Data

A log is created to keep track of unsuccessful attempts to log into the computer. After a person makes five consecutive unsuccessful attempts to log in, all these attempts are recorded in the file **/var/adm/loginlog**. The procedures assume that the file has been created and the operator has logged on as root.

Reviewing User Activity Data Procedure

1 At the UNIX prompt, type **/usr/bin/logins [-admopstux] [-g group..] [-l login..],** then press **Return**.

2 Type **logins -x -l *username,*** then press **Return**.

- Displays login status for a user:

3 Type **/var/adm/loginlog**, then press **Return**. To enable login Logging, this creates the log file **loginlog**.

4 Type **chmod 600 /var/adm/loginlog,** then press **Return**. This sets read and write permissions for root on the file.

5 Type **chgrep sys /var/adm/loginlog,** then press **Return**. This sets the group to **sys**.

Monitoring and Reviewing User Audit Trail Information

The **audit_startup** script is used to initialize the audit subsystem before the audit daemon is started. This script is configurable by the System Administrator, and currently consists of a series of **auditconfig** commands to set the system default policy, and to download the initial events to class mapping. Type the following command to initialize the audit subsystem:

/etc/security/audit_startup

The audit command is the general administrator's interface to the audit trail. The audit daemon may be notified to read the contents of the audit_control file and re-initialize the current audit directory to the first directory listed in the audit_control file or to open a new audit file in the current audit directory specified in the audit_control file as last read by the audit daemon. The audit daemon may also be signaled to close the audit trail and disable auditing. The audit commands are input as shown:

Audit Commands Procedures

1 **audit -n**, then press **Return**.

- Signals audit daemon to close the current audit file and open a new audit file in the current audit directory.

2 **audit -s**, then press **Return**.

- Signals audit daemon to read the current audit file. The audit daemon stores the information internally.

3 **audit -t**, then press **Return**.

- Signals audit daemon to close the current audit file, disable audit and die.

4 **praudit -sl *filename***, then press **Return**.

- Displays audit output. The print audit command converts the binary audit records into a variety of formats, depending on the options used with the commands. The format of audit files is included in the file /usr/include/sys/audit.h. By default, user IDs (UID) and group IDs (GID) are converted to their ACSII representation.

This page intentionally left blank

Practical Exercises

Introduction

These practical exercises are presented in "day-in-the-life" scenarios relating to system administration activities. They represent real situations that you, as system administrator, are likely to encounter on a day-to-day basis.

Equipment and Materials

A functioning ECS computer system.

System Startup and Shutdown

The ECS system was taken down for maintenance earlier in the day and the maintenance has been completed. You must now bring the system to full operation. Turn on the entire ECS system in the prescribed order.

-or-

Bring the following servers to operation:

- SQL Server
- *server 2*
- *server 3*

Tape Operations, System Backup and Restore

1 You have received an approved request from the SEO Chief to perform an incremental backup of the SQL Server for files created or modified within the past 48 hours.

2 Determine how many tapes it will take to back up the required data.

3 Prepare the appropriate number of new tapes to accommodate the backup and perform the label and inventory operations on the tapes.

4 Perform the incremental backup.

5 Inform the SEO Chief that the backup has been performed.

6 ***xuser*** calls you and tells you that she has inadvertently erased the following three files that are critical to her research:

- file1
- file2

- file3

7 She does not remember exactly when they are were last modified. Locate the latest versions of each of the files and perform a file restoration.

User Administration

1 Add the following individual to the system:

UNIX User Registration Request

REQUESTER INFORMATION:

Name: **Erica J. Sonnenshein**

Office Phone Number: **(301) 999-5555**

E-Mail Address: **esonnens@gsfc.nasa.gov** Office Location: **Bldg. 32**

NEW USER INFORMATION:

Name: **Peter Kovalkaides**

Office Phone Number: **(301) 555-1234**

Home Phone Number: **(301) 444-4444**

Organization: **GSFC DAAC**

Group Affiliation(s): **SMC**

Role(s)/Job(s)/Justification: **computer operator with database access required**

Date of Request: **9/17/97** Date Required: **9/22/97**

Supervisor Approval: _____ Date: _____

Ops Supervisor Approval: _____ Date: _____

2 The user you just added has called you with the news that he has forgotten his password. Describe the procedures you must follow to receive authorization to change the individual's password. Assuming you have received the appropriate authorizations, change the password to **gnu-Uzr.**

3 Change the group affiliations for this user to ***new-group affiliation.***

4 Peter Kovalkaides sends you an e-mail message informing that the work on his task is complete and requests that you change the access privileges on all files owned by him to READ ONLY for all classes of users to protect them from changes.

5 You have determined that space on the ***xserver*** is becoming rather scarce. There are a few large files (***insert-file-names-here***) that need to be deleted, and since ***xuser*** and Peter Kovalkaides are done with their projects, their home directories need to be moved to ***insert-new-location-here***. Perform the procedures that will accomplish these tasks assuming you have received the appropriate authorizations. When you are done, inform the affected users of the changes.

New Workstation Installation

Mr. Kovalkaides needs a workstation to do his work. Since the DAAC is just starting up, you'll need to install and configure a new workstation for him.

1 Assign a network name for the workstation.

2 Install the Solaris 2.4 Operating System, the IRIX 5.3 Operating System, or the NCD Operating System as appropriate to this installation.

3 Install ***custom-software-package*** on this machine.

4 Reboot the machine.

5 Log in on this machine and check to see that all processes are operating.

System Log Maintenance

1 The icon on the ECS Desktop for the SQL Server has turned red. Check the system log to find out what the problem is.

2 The problem in the exercise above requires you to restart the SQL server without affecting any of the other subsystems. Perform this task now.

This page intentionally left blank.

Slide Presentation

Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.

This page intentionally left blank.